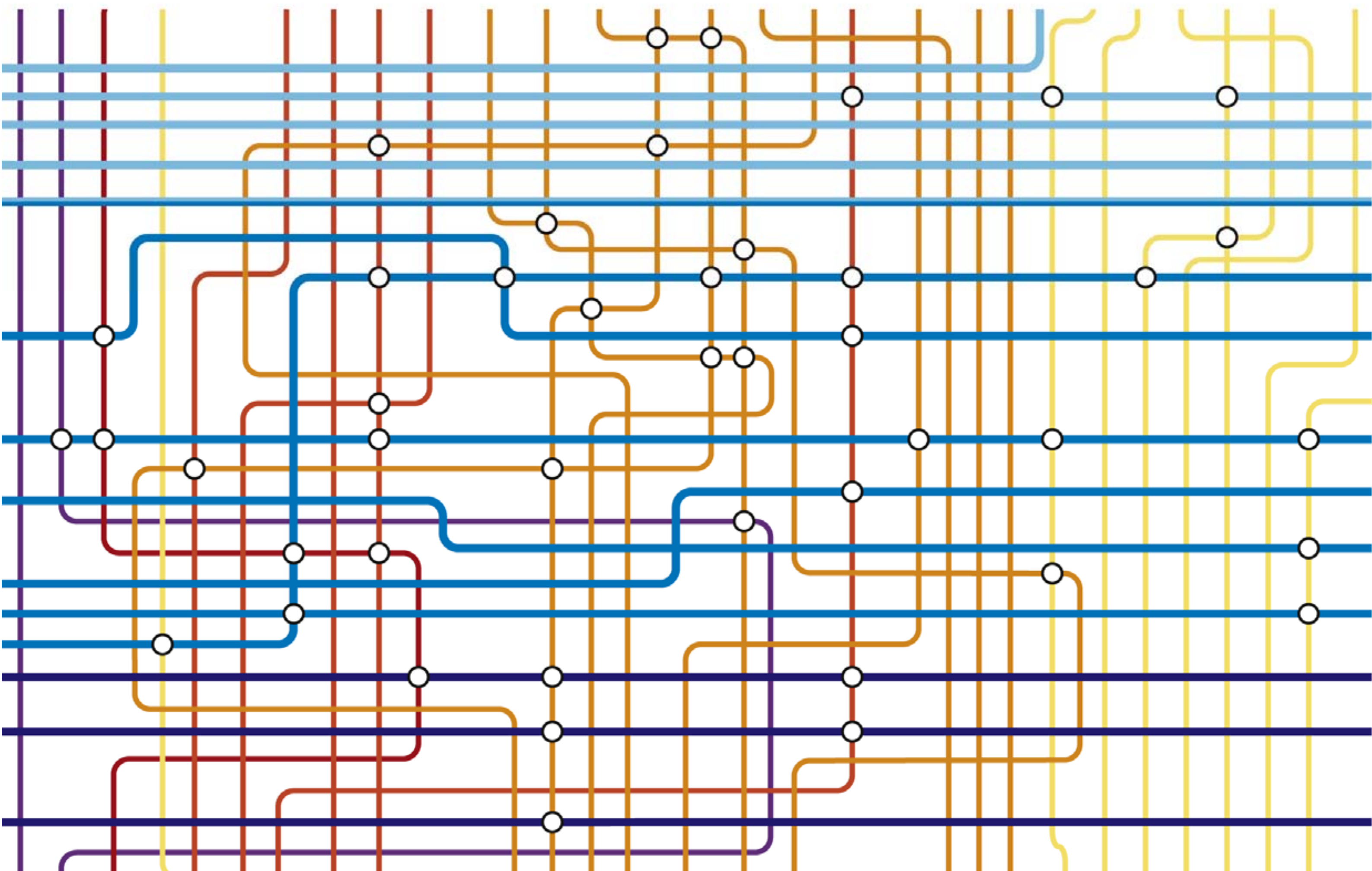
WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID



HAPPY LANDINGS?

HET BIOMETRISCHE PASPOORT ALS ZWARTE DOOS

Vincent Böhre

WEBPUBLICATIE NR. 46

Verkennende studie voor het rapport iOverheid

De voorliggende studie is opgesteld in opdracht van de Wetenschappelijke Raad voor het Regeringsbeleid, meer specifiek de projectgroep Beleid, Informatie en Technologie (BIT). Het vertrekpunt van het WRR-onderzoek dat voor dit project (in deze en andere studies aangeduid als BIT-project) is uitgevoerd, is de zoektocht naar de rol en verantwoordelijkheid van de overheid bij de inzet van ICT. Daarbij richt het project zich meer in het bijzonder op een tweetal vragen: *1) wat zijn de consequenties van de inzet van ICT voor de relatie overheid-burger en welke tendensen zijn daarin zichtbaar? 2) wat is de betekenis van deze consequenties vanuit de verantwoordelijkheid van de overheid wanneer ze ICT inzet in bedrijfsvoering, beleid en beleidsuitvoering?*

Om meer inzicht te verwerven in de dynamiek rondom de ontwikkeling, invoering en het gebruik van ICT in de relatie overheid-burger heeft de projectgroep BIT een aantal empirische studies uitgezet. Daarbij heeft ze de auteurs onder meer gevraagd een aantal beginselen in de analyse te betrekken die als het ware de schragen vormen waarop de relatie overheid-burger in de informatiesamenleving rust. Het betreft de beginselen: keuzevrijheid, identiteit en identificatie, transparantie, effectiviteit en efficiëntie, accountability en privacy.

Om de onderzoeksvragen te kunnen beantwoorden zijn twee typen onderzoek uitgezet bij zowel interne als externe auteurs. De zogenaamde domeinstudies schetsen ontwikkelingen op een breder (beleids)terrein, zoals de zorg, mobiliteit of risicosignalering bij jeugdigen. De zogenaamde black box onderzoeken geven een weergave van de dynamiek op een veel specifieker gebied of rondom een specifieke toepassing binnen een bepaald terrein, zoals biometrie op het paspoort, het EPD of het Veiligheidshuis. Deze black boxen worden in empirische zin 'opengebroken', om de spelers, interacties, verwevenheden en afhankelijkheden die de ontwikkelingen en keuzes sturen, in kaart te kunnen brengen. De hier voorliggende bijdrage vormt een van de extern uitgevoerde onderzoeken. Naast de webpublicaties die in het kader van het project BIT verschijnen, zal het project naar verwachting begin 2011 resulteren in een WRR-rapport aan de regering en een Verkenning. De Verkenning vormt, samen met de webpublicaties en de vele interviews die in het kader van het project BIT gehouden zijn, de empirische onderbouwing voor de aanbevelingen in het te verschijnen WRR-rapport dat de titel 'iOverheid' draagt.

WRR 2010
Omslagillustratie: *Webpagina Zicht op de elektronische overheid*, www.routeplanneregemeente.nl

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

HAPPY LANDINGS?

HET BIOMETRISCHE PASPOORT ALS ZWARTE DOOS

Mr. V. Böhre

Oktober, 2010

Het gedoe met paspoorten blijft (...) een 'black box',
waarmee behalve dan de criminelen niemand is gediend.[*]

We've got a vast coalition of nations that are still with us. They heard the message: either you're with us, or you're not with us. They're still with us. And we're sharing information.[**]

---

* Jan Peter Balkenende (CDA), *Handelingen II*, TK 102, 6613 (Paspoortwet), 14 september 2000.

** President George W. Bush (VS) tijdens zijn ondertekening van de *Enhanced Border Security and Visa Entry Reform Act*, Washington DC, 14 mei 2002.

INHOUDSOPGAVE

TEKSTBOXEN EN FIGUREN

AFKORTINGEN

AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AMv(R)B	Algemene maatregel van (rijks)bestuur
AO	Algemeen Overleg
BPR	Agentschap Basisadministratie Persoonsgegevens en Reisdocumenten
BVD	Binnenlandse Veiligheidsdienst
B&W	Burgemeester en Wethouders
BZ	Ministerie van Buitenlandse Zaken
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CBP	College bescherming persoonsgegevens
CDA	Christen Democratisch Appèl
CRI	Centrale Recherche Informatiedienst
CU	ChristenUnie
D66	Democraten 66
ECID	Expertisecentrum Identiteitsfraude en Documenten
EDPS	European Data Protection Supervisor
EFTD	European Forum for Travel Documents
EHRM	Europees Hof voor de Rechten van de Mens
EU	Europese Unie
EVRM	Europees Verdrag voor de Rechten van de Mens
FBI	Federal Bureau of Investigation
GBA	Gemeentelijke Basisadministratie
HEC	Het Expertise Centrum
ICAO	International Civil Aviation Organization
ICCPR	International Covenant on Civil and Political Rights
ICT	Informatie- en communicatietechnologie
IF4TD	International Forum for Travel Documents
IND	Immigratie- en Naturalisatiedienst
IOM	International Organization for Migration
ISO	International Organization for Standardization
IVBPR	Internationaal Verdrag inzake Burgerrechten en Politieke Rechten
JBZ	Raad Binnenlandse Zaken en Justitie
KLPD	Korps Landelijke Politie Diensten
LIBE	Committee on Civil Liberties, Justice and Home Affairs
LISV	Landelijke Instelling Sociale Verzekering
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
MoU	Memorandum of Understanding
MRP	Machine Readable Passport
MRZ	Machine Readable Zone

MvT	Memorie van toelichting
NBF	Nederlands Biometrie Forum
NCTb	Nationaal Coördinator Terrorismebestrijding
NFI	Nederlands Forensisch Instituut
NGO	Non-gouvernementele organisatie
NGR	Nieuwe Generatie Reisdocumenten
NIK	Nederlandse identiteitskaart
NJCM	Nederlands Juristen Comité voor de Mensenrechten
NRC	Nederlandse Reclame Code
NVVB	Nederlandse Vereniging voor Burgerzaken
OM	Openbaar Ministerie
ORRA	Online Raadpleegbare Reisdocumenten Administratie
OSF	Onafhankelijke Senaats Fractie
OVSE	Organisatie voor Veiligheid en Samenwerking in Europa
PvdA	Partij van de Arbeid
PvdD	Partij voor de Dieren
PVV	Partij voor de Vrijheid
RAAS	Reisdocumenten Aanvraag en Archief Station
RCC	Reclame Code Commissie
RFID	Radio Frequency Identification
SC	Standing Committee
SDU	Staatsdrukkerij en Uitgeverij
SGP	Staatkundig Gereformeerde Partij
TILT	Tilburg Institute for Law, Technology and Society
TNO	Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek
TOV	Taakorganisatie Vreemdelingenzorg
UNHCR	United Nations High Commissioner for Refugees
VKA	Verdonck, Klooster & Associates
VN	Verenigde Naties
VNG	Vereniging van Nederlandse Gemeenten
VS	Verenigde Staten
vtsPN	voorziening tot samenwerking Politie Nederland
VVD	Volkspartij voor Vrijheid en Democratie
VWP	Visa Waiver Program
Wbp	Wet bescherming persoonsgegevens
WRR	Wetenschappelijke Raad voor het Regeringsbeleid

INLEIDING

In het kader van het onderzoek 'Beleid, Informatie en Technologie' (BIT) van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) staat de (veranderende) relatie tussen de Nederlandse overheid en burgers onder invloed van nieuwe informatietechnologie centraal. Deze relatie wordt mede bepaald door de manier waarop door de overheid invulling wordt gegeven aan een aantal fundamentele concepten. De aandacht van de WRR gaat hierbij met name uit naar de volgende beginselen: privacy, identiteit, transparantie, *accountability*, keuzevrijheid, effectiviteit en efficiëntie. Het zijn deze beginselen die de relatie tussen de overheid en de burger in de moderne informatiesamenleving grotendeels bepalen en die deze relatie ook kunnen veranderen of zelfs op scherp kunnen zetten.

Voor WRR-onderzoeksdoeleinden zijn een aantal zogeheten 'socio-technologische systemen' geselecteerd die zich kenmerken door een relatief grote complexiteit en het feit dat deze systemen – bestaande uit de betreffende ICT-toepassing en het relevante samenspel van actoren en belangen daaromheen – relatief slecht gedocumenteerd en moeilijk in kaart te brengen zijn. Eén van deze systemen heeft betrekking op het Nederlandse biometrische paspoort.[1] Doel van dit deelonderzoek is om enig licht te werpen op het biometrische paspoort als maatschappelijk-technologische 'black box' en op de dynamiek die daarbinnen (en ook daaromheen) tot nu toe is opgetreden. Leidende onderzoeksvragen hierbij hebben met name betrekking op relevante Nederlandse actoren, hun doelen en belangen alsmede hun relaties met andere actoren, waaronder met name de burger. Impliciet vormen de genoemde beginselen hierbij de rode draad in het onderzoek; een rode draad die middels tussenconclusies expliciet wordt gemaakt.

Voor dit onderzoek[2] is geprobeerd zo ver mogelijk terug te gaan in de tijd. Dat wil zeggen: tot het moment dat de eerste contouren van het huidige biometrische paspoort zich *publiekelijk* begonnen af te tekenen. Het woord *publiekelijk* is hier bewust benadrukt: veel informatie in het 'biometrische-paspoortdossier' blijkt niet openbaar te zijn. Ook kon in WRR-onderzoekskader slechts een select aantal betrokken personen worden geïnterviewd en heeft de auteur voornamelijk gebruik kunnen maken van (primaire) internetbronnen.

---

1 In het kader van dit onderzoek dient onder het Nederlandse biometrische paspoort tevens de biometrische identiteitskaart te worden begrepen. Dit vanwege de grotendeels parallelle ontwikkeling van beide documenten.

2 Het onderzoek vond grotendeels plaats in de periode november 2009 tot februari 2010 en werd vervolgens met tussenpozen tot augustus 2010 voortgezet.

Mede daardoor bleef het blikveld van dit deelonderzoek relatief algemeen en politiek. Voor een verwante studie naar de technische, industriële en Europese aspecten van het biometrische paspoort wordt de lezer overigens verwezen naar een parallel WRR-deelonderzoek.[3]

3 Zie Max Snijder, *WRR Case Studie: Black Box Biometrisch Paspoort* (nog te verschijnen).

DEEL A *VOICES FROM THE COCKPIT:* DE PARLEMENTAIRE ONTWIKKELING VAN HET BIOMETRISCHE PASPOORT IN VOGELVLUCHT

Het is niet zo dat wij blind zijn, of horende doof voor wat zich in de samenleving afspeelt, maar wij hebben er alles aan gedaan om dit, gegeven dat wat vanuit Europees verband over ons komt, zo goed mogelijk te regelen.[*]

[*] Demissionair staatssecretaris van Binnenlandse Zaken Ank Bijleveld-Schouten (CDA), Vragenuur 20 april 2010, *Handelingen II*, 2009-2010, TK 78, 6606, naar aanleiding van vragen over de nieuwe Paspoortwet.

1 HET BIOMETRISCHE PASPOORT ONDER DE 'PAARSE' KABINETTEN I-II

1.1 De lancering van biometrie in de Nieuwe Generatie Reisdocumenten (1997-2001)

1.1.1 Begin van het ontwikkelingstraject: eerste doelen en betrokkenen

Om het begin van de ontwikkeling van het Nederlandse biometrische paspoort te kunnen traceren dienen we minstens 10 jaar terug in de tijd te gaan: de intentie van de Nederlandse regering om eventueel over te willen gaan tot de invoering van biometrie in paspoorten bleek voor het eerst uit een brief van (destijds demissionair) staatssecretaris van Binnenlandse Zaken Kohnstamm (D66) in december 1997.[1] In deze brief werd het project Nieuwe Generatie Reisdocumenten (NGR) aangekondigd. De Tweede Kamer werd hierover nader geïnformeerd in januari 1998.[2] Doel van het NGR-project was de invoering van gemoderniseerde, beter beveiligde reisdocumenten per 1 januari 2001; dit naar aanleiding van het feit dat het contract tussen het ministerie van Binnenlandse Zaken (namens de staat) en Enschedé/SDU (als ontwikkelaar, producent en distributeur van de toenmalige reisdocumenten) op 31 december 2000 zou aflopen.

Het verkennende (voor)onderzoek van het NGR-project vond plaats van januari t/m mei 1998 en had onder andere betrekking op de vraag naar de noodzaak, wenselijkheid en haalbaarheid van het gebruik van chiptechnologie en biometrie. Hierbij waren deskundigen betrokken van onder meer de Centrale Recherche Informatiedienst (CRI), de Immigratie- en Naturalisatiedienst (IND), de Binnenlandse Veiligheidsdienst (BVD), de ministeries van Defensie (Koninklijke Marechaussee), Buitenlandse Zaken en Justitie, de Vereniging van Nederlandse Gemeenten (VNG) en de Nederlandse Vereniging voor Burgerzaken (NVVB). Geconcludeerd werd dat er behoefte was aan reisdocumenten met chiptechnologie ten behoeve van elektronische identificatie. Ook werd geconcludeerd dat biometrie mogelijkheden zou bieden ter bestrijding van *look-alike* fraude[3] en zou kunnen leiden tot betere dienstverlening aan de burger. De juridische kant van het toepassen van biometrie zou in overleg met de Registratiekamer (het latere College bescherming persoonsgegevens, CBP) verder moeten worden uitgewerkt. Staatssecretaris Kohnstamm achtte grootschalige toepassing van biometrie vooralsnog echter met teveel onzekerheden omkleed (want nog te onbeproefd) en besloot als volgt:

> "Er zal nu verder onderzoek gedaan moeten worden naar alle consequenties. De aspecten privacy en maatschappelijke acceptatie spelen daarbij een belangrijke rol. Het komt mij verstandig voor bij de op te stellen specificaties voor de nieuwe generaties reisdocumenten rekening te houden met de mogelijkheid om biometrie op enig moment toe te passen."[4]

1.1.2 Totstandkoming van het ‘negatieve’ Basisregister Reisdocumenten

In opdracht van het ministerie van Binnenlandse Zaken was in dezelfde periode door Het Expertise Centrum (HEC) onderzoek gedaan naar de noodzaak van het inrichten van een basisregistratie van reisdocumenten. Naar aanleiding hiervan had staatssecretaris Kohnstamm besloten om een zogenaamd ‘negatief’ reisdocumentenregister (van gestolen, vermiste en van rechtswege vervallen documenten) te laten ontwikkelen waarvan Binnenlandse Zaken de eigenaar zou worden.[5] Onder het tweede Kabinet-Kok (‘Paars II’) behoorde dit nieuwe Basisregister Reisdocumenten tot de portefeuille van de minister voor Grote Steden- en Integratiebeleid Van Boxtel (D66). Tijdens de parlementaire behandeling van het wetsvoorstel ter invoering van dit ‘negatieve’ reisdocumentenregister[6] vroeg de VVD waarom niet voor een ‘positief’ register was gekozen.[7] Hierop antwoordde minister Van Boxtel dat een ‘positief’ register “ongetwijfeld voordelen [had]. De inrichting van een dergelijk register [achtte hij] op dit moment echter nog niet opportuun.”[8] Het wetsvoorstel over het Basisregister Reisdocumenten werd begin maart 2001 zonder stemming aangenomen door de Eerste Kamer.[9]

1.1.3 De Nieuwe Generatie Reisdocumenten wordt ‘biometrie-ready’

Intussen was ook het project NGR onder de hoede van minister Van Boxtel gekomen. In het kader van het NGR-project had de minister op 30 maart 1999 aan de Tweede Kamer bericht dat er voor de nieuwe reisdocumenten (in overleg met bovengenoemde instanties[10]) programma’s van technische en beveiligingseisen alsmede functionele- en proceseisen waren opgesteld.[11] Naast CRI en TNO waren deze programma’s van eisen bovendien voorgelegd aan een tweetal buitenlandse instituten, te weten het *Statens Kriminaltekniska Laboratorium* in Zweden en de *Kriminaltechnische Abteilung* van de *Kantonspolizei* in Zwitserland.[12] Tevens had de minister door NIPO Consult (en begeleid door VNG en NVVB) een onderzoek laten uitvoeren naar de mening en wensen van burgers met betrekking tot reisdocumenten. Voor het onderzoek onder burgers was “gebruik gemaakt van een representatieve steekproef van ruim 1000 huishoudens.”[13] Hieruit zou onder andere zijn gebleken “dat de burger ten aanzien van de toepassing van biometrie positief is. Men heeft begrip voor meer geavanceerde technieken die in het kader van de fraudebestrijding worden genomen.”[14] Verder was door HEC (op gezamenlijk verzoek van VNG, NVVB en het ministerie van Binnenlandse Zaken) de besluitvorming omtrent de voorliggende voorstellen onderzocht. De conclusie van HEC zou zijn geweest dat de verschillende stappen in het afwegingsproces zorgvuldig zouden zijn uitgevoerd en dat daarbij rekening zou zijn gehouden met alle relevante aspecten.[15] Ook de minister concludeerde dat “het geschetste afwegingsproces (...) in een open en constructief overleg met VNG en NVVB [had] plaatsgevonden” en “acht[te] het van groot belang dat VNG en NVVB het gedefinieerde beveiligingsniveau voor de nieuwe

reisdocumenten onderschrijven."[16] In 1999 zouden *pilots* worden uitgevoerd om de toepassing van biometrie en elektronische identificatie te beproeven, onder meer in de sociale zekerheidssector, waarbij zou worden samengewerkt met de Landelijke Instelling Sociale Verzekering (LISV) en de Arbeidsvoorziening. Dit met als doel om "begin 2000 meer definitieve voorstellen voor de mogelijke toepassing en de implementatie van biometrie (...) voor te leggen. De specificaties van de nieuwe generatie reisdocumenten worden nu al zodanig opgesteld dat in een later stadium een chip ten behoeve van [biometrie en elektronische identificatie] aan de reisdocumenten kan worden toegevoegd."[17]

Als introductiedatum voor de Nieuwe Generatie Reisdocumenten (na Europese aanbesteding, ontwikkeling, testen, productie en implementatie) bleef 1 januari 2001 in eerste instantie gehandhaafd.[18] Wegens problemen met de ontwikkeling van een zogenaamde 'V-kaart' door Philips Crypto – dat vervolgens failliet ging – trad hierin echter grote vertraging op en werd begin 2001 een nieuwe invoeringsdatum van 1 oktober 2001 bepaald.[19] Het nieuwe paspoort zou dan tevens klaar zijn om ook biometrie in zich op te nemen. Dit gold ook voor de Europese identiteitskaart. In ICAO[20]-verband werd nagegaan of internationaal (ook op Europees niveau) tot afspraken kon worden gekomen. "Nederland moet niet iets gaan doen wat in andere landen afwijkt. (...) Hoewel de minister ook snelheid terzake van de biometrie wenst, moet hij de resultaten van de gesprekken in ICAO-verband afwachten. Technisch gezien kan alles, maar er moet zorgvuldig worden gehandeld."[21] De noodzaak van een biometrisch kenmerk in de reisdocumenten was volgens de minister primair gelegen in de behoefte om de reisdocumenten nog beter te beveiligen, met name tegen *look-alike* fraude. Bovendien bood het de mogelijkheid om ook geautomatiseerde identiteits- en grenscontroles uit te voeren.[22] Over de internationale en Europese context stelde de minister in een brief van mei 2001 het volgende:

> "Om de internationale acceptatie van reisdocumenten te waarborgen stelt de ICAO richtlijnen vast. De richtlijnen hebben geen dwingend karakter, maar bieden wel waarborgen voor acceptatie van reisdocumenten door andere landen. De richtlijnen die door de Europese Unie worden gesteld aan reisdocumenten zijn ontwikkeld met inachtneming van de ICAO-normen die daardoor een integraal onderdeel uitmaken van de EU-normen. Vanzelfsprekend wordt in Nederland bij de ontwikkeling van reisdocumenten rekening gehouden met de EU-eisen en ICAO-richtlijnen. Overigens maakt de eventuele toepassing van biometrie in reisdocumenten van de lidstaten thans geen onderdeel uit van de EU-agenda. (...) Ten aanzien van biometrie is de ICAO al enige tijd, *in nauwe samenwerking met het bedrijfsleven*, actief. Dat is vooral ingegeven door het feit dat een aantal landen, waaronder Nederland, Canada, de Verenigde Staten en Nieuw Zeeland het gebruik van biometrie in reisdocumenten overwegen. (...) Alhoewel op dit moment geen enkele biometrische techniek voor de toepassing in reisdocumenten kan worden uitgesloten komt ICAO tot de voorlopige conclusie dat gezichtherkenning, vingerafdruk en irisherkenning het meest geschikt zijn om in de reisdocumenten op te nemen. Thans wordt onderzocht of de drie technieken in een praktische toepassing kunnen worden getest. Op basis van de resultaten van die proeven zal ICAO komen met een aanbeveling voor een biometrisch kenmerk voor reisdocumenten. Mijn verwachting is dat de ICAO in 2003 de richtlijnen voor biometrie in reisdocumenten zal vaststellen."[23]

1.1.4 Juridisch kader rond het gebruik van biometrie

Het juridische kader rond de gerechtvaardigde verwerking van biometrische kenmerken in reisdocumenten werd volgens de minister bepaald door het Europees Verdrag voor de Rechten van de Mens (EVRM, art. 8), de Grondwet (art. 10), de Europese Privacyrichtlijn, de Wet bescherming persoonsgegevens (Wbp) én een belangwekkend rapport van de Registratiekamer over biometrie, getiteld *At face value*.[24] In dit kader achtte de minister tevens relevant dat "de verspreiding van het [biometrische] gegeven wordt tegengegaan, enerzijds door de *decentrale opslag in de chip zelf* en anderzijds doordat het gegeven bij verificatiehandelingen niet in bestanden van verificerende instellingen wordt opgenomen."[25] De minister voegde hier echter aan toe dat "overwogen wordt het biometrisch kenmerk toe te voegen aan de andere persoonsgegevens die opgeslagen worden in de reisdocumentenadministratie. Deze administratie dient ter raadpleging in geval van vermissing en andere bijzondere omstandigheden in het gebruik van reisdocumenten."[26]

Tekstbox 1.1

In september 1999 publiceerde de Registratiekamer (het latere CBP) het rapport *At face value: on biometrical identification and privacy*.[27] Dit rapport beoogde een richtinggevend kader te bieden voor verantwoord gebruik van biometrie en formuleerde daartoe een achttal kernvragen[28]:

1) Welke gegevens zijn echt nodig voor het doel?
2) Worden de gegevens rechtmatig ingewonnen? Is de betrokken persoon volledig geïnformeerd, ook over het doel waarvoor de gegevens worden gebruikt?
3) Is er sprake van 'gevoelige gegevens'? (Bijvoorbeeld in verband met etniciteit of gezondheid.)
4) Wat gebeurt er met de oorspronkelijke biometrische gegevens? Worden deze verwijderd?
5) Zijn de biometrische gegevens zo opgeslagen dat ze niet meer terug te voeren zijn tot de oorspronkelijke gegevens?
6) Is het mogelijk om de meting van de gegevens en de verificatie decentraal te laten plaatsvinden?
7) Is de beveiliging van *templates* voldoende?
8) Rechtvaardigt het doel een eventuele centrale opslag van biometrische gegevens?

Het rapport benadrukte tevens dat biometrische identificatiesystemen technisch zo dienden te worden ingericht dat slechts een minimale hoeveelheid persoonsgegevens zou worden ingewonnen en dat de verspreiding van die gegevens voorkomen werd. Het rapport stelde in dit verband onder andere dat "[a]s a rule both the storage of templates and the verification process should be decentralised. (...) The original biometrics should preferably be destroyed after the derivation of the digital template (...)."[29]

1.1.5 Onderzoeken en *pilots*

In het kader van twee lopende haalbaarheidsstudies rond de invoering van biometrie en elektronische identificatie waren door de minister diverse onderzoeken en *pilots* gepland. Uit een onderzoek van bureau Ernst & Young Forensic Services zou inmiddels zijn gebleken dat invoering van biometrie wenselijk was en een bijdrage zou kunnen leveren aan het beperken van *look-alike* fraude. Ook waren er reeds enkele lokale *pilots* gestart met vingerscans in identiteitskaarten en reisdocumenten ter identificatie bij elektronische dienstverlening door de overheid (onder andere in het kader van sociale zekerheid); het eerste verloop van deze *pilots* bleek echter vrij moeizaam. Voor de tweede helft van 2001 waren door de minister tevens enkele biometrische *pilots* met irisscans en gezichtsherkenning voorzien. Hierbij waren de volgende organisaties betrokken: de Taakorganisatie Vreemdelingenzorg (TOV), de Vreemdelingendienst, luchthaven Schiphol, Koninklijke Marechaussee, IND, het ministerie van Binnenlandse Zaken en de Registratiekamer. Verder vonden er gesprekken over mogelijke *pilots* met de bancaire sector en de zorgsector plaats. Naast deze kleinschalige *pilots* werden tevens enkele grootschalige proeven gepland voor begin 2002, waaronder in samenwerking met banken, de zorgsector, LISV en Arbeidsvoorziening Nederland. Een en ander was er op gericht om in de tweede helft van 2002 tot definitieve conclusies te kunnen komen over de vraag of grootschalige invoering van biometrie en elektronische identificatie mogelijk zou zijn.[30]

1.2 Tussentijdse vluchtimpressie, zomer 2001: *all passengers happy*

1.2.1 Haastige spoed in de Tweede Kamer

Een tussentijds Algemeen Overleg (AO) in de Tweede Kamer dat hier als representatief voorbeeld kan worden uitgelicht dateert van 21 juni 2001,[31] naar aanleiding van de brief van de minister een maand eerder.[32] Bij dit AO deden diverse Kamerleden onder meer verslag van hun recente werkbezoek aan Johan Enschedé en SDU. De teneur van de politieke discussie was dat men enthousiast was en dat een en ander haast had. Enkele citaten: “De heer Zijlstra (PvdA) toont zich na een bezoek aan Joh. Enschede en de SDU zeer onder de indruk van de geavanceerde ontwikkelingen en vele mogelijkheden op het terrein van de biometrie. (...) De heer De Swart (VVD) is na een bezoek aan Joh. Enschede en de SDU ook onder de indruk van de mogelijkheden met biometrie. Met name de vingerscan en irisscan zijn al behoorlijk ver in ontwikkeling. (...) Misschien moet Nederland overwegen een voortrekkersrol te vervullen en vooruitlopend op andere Europese landen biometrische kenmerken invoeren. (...) De heer Balkenende (CDA) constateert, na zijn bezoek aan de SDU en Johan Enschede, dat het indrukwekkend is om te zien wat er technisch allemaal kan en gebeurt. (...) De CDA-fractie vindt het opnemen van biometrische kenmerken (...) urgent en dringt aan op spoed. (...) De

heer Balkenende constateert dat het opnemen van een biometrisch kenmerk wijziging van artikel 3 van de Paspoortwet noodzakelijk maakt. Dit is een technische verbetering, geen principiële wijziging. (...) De heer Balkenende hoopt dat bij deze noodzakelijke technische verbetering, de privacy geen belemmering zal gaan vormen. De maatschappelijke acceptatie is ook van groot belang. Nederlanders begrijpen in het algemeen wel dat het vanwege de veiligheid [van biometrie meer] tijd [zal gaan] kost[en] om reisdocumenten te krijgen. (...) Het is zinvol om (...) *pilots* te doen, maar zij mogen geen belemmering vormen voor dat wat echt nodig is, namelijk het opnemen van biometrische kenmerken in een reisdocument. (...) De heer Balkenende verzoekt de minister te bevestigen dat bij artikel 3 van de Paspoortwet het privacyaspect niet aan de orde is, maar dat het gaat om een technisch kenmerk dat in de wet moet worden opgenomen. De wet biedt het algemene kader en de technische zaken worden via AMvB geregeld. Zo hoort het. Op voorhand krijgt de minister daarbij steun van de CDA-fractie."[33]

1.2.2 Geduld op regeringsniveau

Ook de minister "was bij zijn bezoek aan Joh. Enschede/SDU onder de indruk (...). De minister constateert [echter] dat in dit proces ongeduld wel aan wijsheid gekoppeld moet worden. (...) Ook de privacyaspecten spelen een rol. Daarom is gekozen voor een aantal *pilots* met vingerafdruk, met irisscan en met gelaatsherkenning. (...) Bij de irisscan is er geen koppeling met raskenmerken. Bij gelaatskenmerken zou dat mogelijk zijn. Er wordt op gelet dat een en ander niet discriminerend kan werken. (...) Redelijkerwijs is de verwachting dat [biometrie] in 2004 in het paspoort kan worden opgenomen. (...) Desgevraagd zegt de minister toe dat hij contact met zijn collega van Justitie zal opnemen, om te zien of Nederland dit onderwerp op de EU-agenda kan krijgen. (...) De minister vindt het draagvlak onder de bevolking een interessant punt. Onlangs is op het departement een onderzoek hiernaar aan de orde geweest. De minister heeft ook nauw contact met de Registratiekamer. De acht vragen in het rapport *At face value* zijn voortdurend leidraad bij de opzet van de *pilot*s en de evaluatie. (...) De minister constateert dat biometrie dient ter vaststelling van de identiteit en niet betekent dat iemand een leven lang gevolgd wordt. De Registratiekamer zit er ook bij om te bewaken dat er geen verkeerde dingen met gegevens worden gedaan (...). De minister hoopt ten slotte dit najaar een onderzoek naar het draagvlak onder de bevolking te starten."[34]

1.3 CDA-proefballon over opslag van vingerafdrukken crasht tijdens opstijgen

De gebeurtenissen van 11 september 2001 brachten de ontwikkeling van biometrie wereldwijd in een stroomversnelling. Zo ook in Nederland, waar het CDA op 4 december 2001

publiekelijk het idee lanceerde om alle volwassen Nederlanders hun vingerafdrukken te laten afstaan om het opsporen van misdrijven gemakkelijker te maken:

> "CDA-Kamerlid Joop Wijn wilde dit vandaag voorstellen tijdens een debat over het gebruik dat de politie maakt van de vingerafdrukken van asielzoekers. Minister Benk Korthals van Justitie moet de Tweede Kamer daar uitleg over geven. Volgens de huidige uitleg van de privacywetgeving mag [het] niet. (...) Volgens Wijn is er geen bezwaar tegen het verzamelen van de vingerafdrukken, omdat daaruit geen gegevens over bijvoorbeeld gezondheid zijn af te leiden. Dat is volgens hem ook het verschil met het opslaan van DNA-materiaal van alle Nederlanders. 'Dit is louter voor de identificatie.' *Het afnemen van de vingerafdrukken zou kunnen samenvallen met het afhalen van een paspoort.* D66-Kamerlid Boris Dittrich is tegen deze uitbreiding. Volgens hem mogen vingerafdrukken alleen worden afgenomen bij verdenking van een strafbaar feit. 'Anders gaan we naar een Big Brother-maatschappij.' De VVD is sceptisch. 'Het is nuttiger meer gebruik te maken van DNA,' zegt VVD-Kamerlid Atzo Nicolaï. 'Dit is het paard achter de wagen spannen.' Het is volgens hem ook niet nuttig allerlei gegevens vast te leggen van alle Nederlanders; dat moet alleen gebeuren bij mensen die zijn veroordeeld. Ook bij de PvdA kan het voorstel van Wijn op weinig enthousiasme rekenen."[35]

Het opslaan van de vingerafdrukken van alle Nederlanders was "nauwelijks privacygevoelig", aldus Wijn.[36] "Een vingerafdruk zegt niets over iemands aanleg voor ziekten, over iemands financiële positie of over iemands gedrag op bijvoorbeeld internet. (...) Je kunt zoiets gewoon netjes regelen."[37] Wijn werd hierin gesteund door professor Ronald Plasterk die enkele dagen later te gast was in het televisieprogramma Buitenhof:

> "Paul Witteman zal gisteren in Buitenhof wel met enige afgunst naar de performance van Ronald Plasterk hebben gekeken. Plasterk legde glashelder uit waarom het aanleggen van een nationaal bestand met vingerafdrukken of met DNA-fingerprints geen inbreuk op de privacy is. Daarvoor gebruikte hij de slimme vergelijking met het opschrijven van de beginletters van de eerste twintig bladzijden uit een boek. Daarmee kan een boek worden geïdentificeerd, maar het zegt niets over de inhoud. Aan het slot van zijn betoog voegde Plasterk de daad bij het woord, schraapte met een wattenstaaf wat DNA-materiaal uit zijn mond en beloofde dat over een paar dagen op de website van Buitenhof zijn DNA-profiel [zou] staan."[38]

De avond ervoor was het onderwerp ook behandeld in het televisieprogramma Het Lagerhuis:

> "Daar trad CDA-Kamerlid Joop Wijn op als pleitbezorger van een landelijke databank met vingerafdrukken. Wijn bracht zijn standpunt verdienstelijk naar voren, maar miste de scherpte van Plasterk om de tegenstanders van zo'n databank krachtig van repliek te dienen. Een paar discussianten riepen het schrikbeeld van de politiestaat op (...)."[39]

Nog geen week nadat het CDA deze proefballon had gelanceerd, maakte minister Korthals van Justitie (VVD) er echter korte metten mee:

> "... [I]n antwoord op de vraag van het lid Wijn van Uw kamer [ben ik] niet bereid om van alle Nederlanders vingerafdrukken te nemen in het belang van de opsporing. Dit middel is buitenproportioneel gelet op bijvoorbeeld het aantal aangeboden sporenzaken op jaarbasis, in geheel Nederland ca. 10.000. Voorts is het praktisch onuitvoerbaar omdat alle tien de vingers en eventueel de handpalmen moeten worden afgenomen, wil het zinvol zijn voor de opsporing. Dat vergt een te groot beslag op de capaciteit van de politie. Dit nog afgezien van de administratieve verwerking en controle. In het kader van het nieuwe identiteitsbewijs wordt

> mogelijk een biometrisch kenmerk opgenomen zoals bijvoorbeeld een vingerafdruk. Daar gaat het er om te bepalen dat de bezitter van het identiteitsbewijs ook daadwerkelijk [de] persoon is die op dat bewijs staat vermeld. Daarvoor is wellicht één vingerafdruk voldoende, dat is echter volstrekt onvoldoende voor de opsporing."[40]

Het CDA reageerde hierop echter onverminderd vastberaden:

> "[Het CDA] vindt (...) dat er een meer algemene bereidheid moet worden geconstrueerd voor het afstaan van vingerafdrukken, want dat verhoogt het oplossingspercentage. In de brief van de minister worden daar praktische argumenten tegen ingebracht, zoals het aantal aangeboden sporenzaken, het aantal vingers en de politiecapaciteit, maar geen principiële. Wat [de CDA-fractie] betreft hoeft deze kwestie overigens niet voor het kerstreces te worden gerealiseerd. *Het verkrijgen van alle vingerafdrukken mag best een paar jaar duren. Dit kan worden gekoppeld aan het ophalen van een identiteitsbewijs. Dat past in het streven te komen tot een algemene identificatieplicht.*"[41]

Desgevraagd wees Joop Wijn een verzoek om een interview door de WRR over het biometrische paspoort tweemaal af.[42]

1.4 Intermezzo: overzicht van geïnterviewde personen

Zoals reeds opgemerkt in de inleiding kon voor WRR-onderzoeksdoeleinden slechts een (zeer) select aantal personen door de auteur worden geïnterviewd. Deze kleine groep mensen bestond voornamelijk uit (deels voormalige) ambtenaren die meerdere jaren nauw betrokken zijn (geweest) bij de ontwikkeling van het Nederlandse biometrische paspoort. Alle geïnterviewden spraken op persoonlijke titel. Op één interview na (bij Sagem, voorheen SDU) zijn de schriftelijke verslagen van alle interviews geaccordeerd (zie tabel 1.1).

Door middel van 'intermezzo's' in de tekst van deze rapportage zullen relevante fragmenten van de interviews worden uitgelicht, te beginnen met enkele opmerkingen over de zojuist beschreven periode. Uit meerdere interviews bleek in dit verband dat het idee voor de invoering van vingerafdrukken in reisdocumenten reeds bestond sinds eind jaren 90. Volgens Jan Grijpink berustte dit destijds echter op een misverstand:

> "[Bij SDU had men] het idee dat je met de vingerafdrukken van de houder een nieuwe generatie veiligheidskenmerken van het document kon introduceren. [Men gaf bij SDU] uiteindelijk [echter] toe dat dat idee op een denkfout berustte. Het document zou er niet beter van worden, maar juist meer een doelwit voor kwaadwillenden. Daardoor zou het per saldo in het gebruik worden verzwakt."[43]

Tabel 1.1 Overzicht interviews

	Organisatie	Functie	Datum interview
Fons Knopjes[44]	ID Management Centre	Dhr. Knopjes is *managing director* van het ID Management Centre te Den Haag. Voorheen was hij onder meer falsificatiespecialist bij de Centrale Recherche Informatiedienst (CRI) en *R&D manager* bij het agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR, ressorterend onder het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)). Tevens was dhr. Knopjes bestuurslid en voorzitter van het Nederlands Biometrie Forum (NBF).	1 december 2009
Jan Grijpink[45]	ministerie van Justitie, NBF	Dhr. Grijpink is raadadviseur informatiestrategie bij het ministerie van Justitie, hoogleraar Informatiekunde aan de Universiteit Utrecht, adviseur van Het Expertise Centrum (HEC) en voorzitter van het NBF.	3 december 2009
Gerard Paalman	Sagem Identification	Dhr. Paalman is hoofd Productontwikkeling bij Sagem te Haarlem. Voorheen was hij werkzaam bij SDU (onder meer als projectmanager NGR). Ook was hij secretaris van het NBF.	7 januari 2010 (ongeaccordeerd)
Ron van Troost[46]	NVVB	Dhr. Van Troost is senior beleidsmedewerker bij de Nederlandse Vereniging voor Burgerzaken (NVVB) te Zoetermeer, onder andere op het terrein van identiteitsdocumenten.	27 januari 2010
Peter Provily & Paul van der Zanden[47]	ministerie van BuZa	Dhr. Provily is hoofd Programma- en Projectmanagement binnen de Centrale Directie Informatiseringsontwikkeling van het ministerie van Buitenlandse Zaken (BZ). Voorheen was hij bij BZ projectleider biometrie vanuit het Directoraat Generaal Regiobeleid en Consulaire Zaken. Dhr. Van der Zanden is coördinerend beleidsmedewerker bij de Directie Consulaire Zaken en Migratiebeleid en was voorheen projectmanager biometrie bij BZ.	4 februari 2010
Ruud van Munster[48]	TNO, NBF	Dhr. Van Munster is *senior consultant public security* bij TNO Defence, Security & Safety en *senior business consultant* bij TNO. Hij is tevens mede-oprichter en bestuurslid van het NBF.	16 februari 2010
Edwin Delwel & Edwin Koedam[49]	vtsPN	Dhr. Delwel en dhr. Koedam zijn respectievelijk commissaris van politie bij de Divisie Informatievoorziening & Technologie en teamcoördinator bij de Vraagunit Ketencoördinatie van de voorziening tot samenwerking Politie Nederland (vtsPN) te Zeist.	17 februari 2010
Arnout Ruifrok[50]	NFI	Dhr. Ruifrok is wetenschappelijk onderzoeker op het gebied van beeldonderzoek en biometrie bij het Nederlands Forensisch Instituut (NFI) te Den Haag. Tevens is hij in justitiekader actief als gezichtsvergelijkingsexpert bij PROMIS (Project motiveringsverbetering in strafvonnissen).	18 februari 2010
Henk Kooij & Mark Levering[51]	ECID	Dhr. Kooij en dhr. Levering zijn respectievelijk werkzaam als hoofd en als operationeel analist van de afdeling Criminaliteitsanalyse van het Expertisecentrum Identiteitsfraude en Documenten (ECID) te Schiphol.	27 april 2010

Sindsdien is desondanks een kleine groep van veelal dezelfde personen direct betrokken geweest bij de Nederlandse ontwikkeling van het biometrische paspoort en de (latere) opslag van biometrie, zowel van de zijde van de overheid (BZK, agentschap BPR en Justitie) als vanuit

de industrie (SDU, het latere Sagem). “Het was verder een voortdurende wisselwerking tussen een kleine (en deels dezelfde) groep mensen op nationaal, Europees en internationaal niveau,” zo vertelt Jan Grijpink.[52] Door Fons Knopjes wordt aangevuld dat deze situatie in wezen tot de dag van vandaag voortduurt: “[d]eze business wordt gedomineerd door een heel klein kringetje.”[53] Wat dit ‘kringetje’ betreft springt vooral het Nederlands Biometrie Forum (NBF) in het oog, niet in de laatste plaats vanwege de posities van een aantal geïnterviewden binnen en buiten dit Forum. Volgens diezelfde geïnterviewden zou het NBF bij de ontwikkeling van het biometrische paspoort echter vrijwel geen rol hebben gespeeld.[54] Het NBF zou zich slechts eenmaal actief hebben opgesteld, naar aanleiding van het latere besluit om een centrale biometrische database te ontwikkelen: “daarover heeft het NBF informeel vragen gesteld aan de toenmalige beleidsverantwoordelijke van BPR; zeer kritische vragen over de toegankelijkheid van die database,” aldus Ruud van Munster.[55] Van Munster voegt tevens toe dat het NBF “nooit een standpunt [heeft] ingenomen in het publieke debat (voorzover daarvan sprake was) over het biometrische paspoort; het NBF had ook nooit die intentie.”[56] Verder had (en heeft) het NBF volgens Ron van Troost op het terrein van het biometrische paspoort “hooguit een indirecte rol, in verband met de mogelijke (bedrijfsmatige) toepassingen van biometrie in het algemeen en de levensvatbaarheid daarvan. Ik zie het NBF vooral als een organisatie die goed is in het delen van kennis over de huidige ontwikkelingen en mogelijkheden op dit terrein.”[57]

1.5 Tussenconclusie

In de ‘vroege’ parlementaire geschiedenis van het biometrische paspoort vallen een aantal zaken op. Allereerst leek er sprake te zijn van relatieve *openheid* over de (overheids)actoren die bij de ontwikkeling van het biometrische paspoort betrokken waren (zeker in vergelijking tot de parlementaire jaren die nog zouden volgen), al zou dit tot ‘9/11’ slechts een klein aantal organisaties (waaronder met name SDU, BZK, agentschap BPR en Justitie) betreffen. Hoewel de verschillende belangen en agenda’s van alle betrokkenen grotendeels in het ongewisse bleven, verkreeg de burger zo tenminste enig zicht op ‘het veld en de spelers’. Ook werd diezelfde burger ingelicht over de betrokkenheid van enkele buitenlandse instituten alsmede over reeds gedane en nog uit te voeren externe onderzoeken en *pilots*, waaronder ‘zelfs’ een onderzoek naar de eigen besluitvorming van de overheid. (Dit alles ondanks de natuurlijke terughoudendheid in transparantie van overheidswege op het politiek gevoelige terrein van het paspoort. Deze terughoudendheid gold met name sinds de paspoortaffaire van eind jaren 80.) Hierbij dient echter te worden aangetekend dat géén van de genoemde onderzoeken voor een breed publiek beschikbaar werd gesteld. Hierdoor kon de burger dus slechts afgaan op wat de minister op basis van deze onderzoeken meende te kunnen concluderen. Ook bleven (mogelijk) relevante private, industriële partijen (op Johan Enschedé en SDU na) voor

de burger vrijwel geheel buiten beeld. Een uitzondering vormde de bancaire sector, die in de wetsgeschiedenis enkele keren nadrukkelijk werd genoemd.

Een tweede opvallend punt betreft het relatief grote belang wat van overheidswege leek te worden gehecht aan de *privacy* van de individuele burger. Zowel het relatief brede scala aan relevant geachte juridische instrumenten als de structurele betrokkenheid van de Registratiekamer getuigden hiervan. Dit overigens in tegenstelling tot de Tweede Kamer (met name het CDA), waar het recht op privacy nauwelijks een rol leek te spelen en welhaast sprake leek te zijn van een blind geloof in biometrie. Symptomatisch was in dit verband dan ook het voorstel van het CDA om de vingerafdrukken van alle Nederlanders (middels het paspoort) op te slaan voor opsporingsdoeleinden; iets waar de meeste andere politieke partijen en de betrokken minister tegen bleken te zijn.

Aan maatschappelijke acceptatie van biometrie leek door de verantwoordelijke bewindspersonen de nodige waarde te worden gehecht; in die zin leek er impliciet dan ook nog sprake te zijn van enige '*keuzevrijheid*' (in ruime zin) aan de kant van de bevolking. Gezien het politieke momentum dat de ontwikkeling van het biometrische paspoort reeds leek te hebben, kan men zich echter afvragen in hoeverre eventueel gebleken weerstand onder de bevolking een en ander destijds nog zou hebben kunnen tegenhouden. Aan eventuele keuzevrijheid in enge zin (dat wil zeggen voor de individuele burger) werd bovendien in het geheel geen aandacht besteed; het eventueel behouden van een conventioneel alternatief voor het biometrische paspoort (bijvoorbeeld voor principieel bezwaarden) was geen onderwerp van politieke discussie. Overigens leek voor de invoering van het biometrische paspoort als zodanig en voor de in dat paspoort op te nemen biometrische kenmerken ook een gebrek aan effectieve keuzevrijheid te gelden voor de Nederlandse staat als geheel, gezien de internationale en Europese ontwikkelingen terzake. Na '9/11' leek (ook) op dit terrein immers 'go with the flow' het motto.

Een ander beginsel dat (nog) minder scherp in beeld kwam had betrekking op *accountability*. Weliswaar lag de (aanwijsbare) politieke verantwoordelijkheid voor de ontwikkeling van het biometrische paspoort in de geschetste periode achtereenvolgens bij de staatssecretaris van Binnenlandse Zaken en bij de minister voor Grote Steden- en Integratiebeleid, de juridische aspecten van het biometrische paspoort dienden echter nog verder te worden uitgewerkt in overleg met de Registratiekamer. Wel was er als gezegd sprake van diverse onderzoeken en *pilots*, ook met betrekking tot het draagvlak onder de bevolking en de besluitvorming. In het algemeen leken de verantwoordelijke bewindspersonen – in tegenstelling tot sommige politieke partijen – op dit terrein dan ook niet over één nacht ijs te willen gaan.

De beginselen *effectiviteit* en *efficiëntie* kwamen slechts impliciet (en amper besproken, laat staan publiekelijk aangetoond) in beeld als zijnde als het ware inherent aan de (beleids)doelen die voor de invoering van het biometrische paspoort achtereenvolgens werden gesteld: modernisering en betere beveiliging van het paspoort, elektronische identificatie, bestrijding van (*look-alike*) fraude, betere (elektronische) dienstverlening aan de burger en geautomatiseerde identiteits- en grenscontrole. Op het voorstel van het CDA na was van eventuele strafrechtelijke doelen in het geheel nog geen sprake.

Over het beginsel *identiteit* kan vooralsnog worden opmerkt dat dit in wezen de onderliggende rode draad is van het gehele 'biometrische-paspoortdossier'. In essentie is dit hét concept waar alles op het terrein van biometrie om draait. Des te opvallender is het dan ook dat het concept 'identiteit' op dit terrein veelal slechts in zijn meest beperkte en kunstmatige vorm leek (en lijkt) te worden opgevat: als relatief willekeurige verzameling oppervlakkige kenmerken van een bepaald individu. (De mens als 'biometrisch getal'.) In dat beperkte mensbeeld leek (en lijkt) voor de problematiek van principieel bezwaarden per definitie geen plaats. Bovenstaande constatering over het gebrek aan keuzevrijheid lijkt hier mee samen te hangen.

Noten

1 Zie de brief van de staatssecretaris van Binnenlandse Zaken (Jacob Kohnstamm; D66) d.d. 9 december 1997, *Kamerstukken II*, 1997-1998, 25764, nr. 3, p. 4. Zie in dit verband tevens de nota 'Wetgeving voor de elektronische snelweg' (12 februari 1998), *Kamerstukken II*, 1997-1998, 25880, nr. 2, pp. 129-130, 142. In deze nota kondigde de regering aan het gebruik van biometrie door en binnen de overheid te willen bevorderen als onderdeel van een breed beleidsprogramma voor betrouwbaar elektronisch rechtsverkeer.

2 Zie de brief van de staatssecretaris van Binnenlandse Zaken (Jacob Kohnstamm) d.d. 15 januari 1998, *Kamerstukken II*, 1997-1998, 25764, nr. 4. Naar aanleiding hiervan werden tijdens het Algemeen Overleg op 24 maart 1998 slechts door een handjevol Kamerleden (onder wie Remkes (VVD) en Verhagen (CDA)) vragen gesteld, waaronder over biometrie; zie *Kamerstukken II*, 1997-1998, 25764, nr. 5. Een andere opvallende naam in deze 'vroege' parlementaire geschiedenis is die van Kamerlid Bijleveld-Schouten (CDA), bijvoorbeeld in verband met de toenmalige (vernieuwde) generatie paspoorten: eind november 1997 had zij staatssecretaris Kohnstamm gevraagd om de Kamer schriftelijk te informeren over de gang van zaken rond de nieuwe beveiligingskenmerken in deze paspoorten en de terzake uitgebrachte rapporten en adviezen. Zie de brief van de staatssecretaris van Binnenlandse Zaken (Jacob Kohnstamm) d.d. 9 december 1997, *Kamerstukken II*, 1997-1998, 25764, nr. 2.

3 *Look-alike* fraude is een vorm van misbruik waarbij iemand een authentiek (reis)document gebruikt van een ander waarmee hij of zij uiterlijke gelijkenis vertoont. Deze vorm van fraude neemt toe naarmate documenten beter beveiligd zijn tegen 'traditionele' vormen van fraude, zoals vervalsing. Zie hierover bijv. F. Knopjes & D. Ombelli, *Documents: The Developer's Toolkit* (IOM, 2008), pp. 49-50.

4 Brief van de staatssecretaris van Binnenlandse Zaken (Jacob Kohnstamm) d.d. 12 juni 1998, *Kamerstukken II*, 1997-1998, 25764, nr. 7, p. 5.

5 Ibid., p. 8. Dit HEC-onderzoek was "ter inzage gelegd bij de afdeling Parlementaire Documentatie"; ibid., p. 2.

6 Wijziging van de Paspoortwet, onder andere in verband met het daarin opnemen van enige bepalingen ter voorkoming van misbruik van reisdocumenten, *Kamerstukken II*, 1999-2000, 26977, nrs. 1-2 (21 januari 2000).

7 Zie het verslag van de vaste commissie voor Binnenlandse Zaken, *Kamerstukken II*, 1999-2000, 26977, nr. 4 (7 maart 2000), p. 2.

8 Nota van de minister voor Grote Steden- en Integratiebeleid (Roger van Boxtel) d.d. 6 juni 2000, *Kamerstukken II*, 1999-2000, 26977, nr. 6, p. 9.

9 Zie *Handelingen I*, 2000-2001, 21-983 (6 maart 2001). Hierna volgde publicatie in Staatsblad 2001, 132.

10 Zie *supra*, paragraaf 1.1.1.

11 Zie de brief van de minister voor Grote Steden- en Integratiebeleid (Roger van Boxtel) d.d. 30 maart 1999, *Kamerstukken II*, 1998-1999, 25764, nr. 10, p. 4.

12 Zie ibid.

13 Ibid., p. 5.

14 Ibid.

15 Zie ibid. Dit HEC-onderzoek was "ter inzage gelegd bij de afdeling Parlementaire Documentatie"; ibid.

16 Ibid.

17 Ibid., p. 7.

18 Ibid.

19 Zie Algemeen Overleg met minister Van Boxtel d.d. 24 januari 2001, *Kamerstukken II*, 2000-2001, 25764, nr. 15, pp. 2-4. Overigens stelde Kamerlid Balkenende (CDA) tijdens dit overleg dat "pas een echt goede slag kan worden geslagen als de biometrische kenmerken in het paspoort zitten. (...) Hoe eerder die kenmerken kunnen worden toegevoegd, hoe beter." Ibid., p. 2.

20 International Civil Aviation Organization.

21 Ibid., pp. 3-4.

22 Zie de brief van de minister voor Grote Steden- en Integratiebeleid (Roger van Boxtel) d.d. 11 mei 2001, bzk 01-535, p. 2.

23 Ibid., p. 3 (cursivering VB).

24 Zie ibid., pp. 3-4.

25 Ibid., p. 4 (cursivering VB).

26 Ibid.

27 Registratiekamer, *At face value: on biometrical identification and privacy* (Den Haag, september 1999); beschikbaar op www.cbpweb.nl/Pages/av_15_At_face_value.aspx.

[28] Zie ibid., pp. 59-60, 72.

[29] Ibid., p. 60.

[30] Zie de brief van minister Van Boxtel d.d. 11 mei 2001, *supra* noot 22, pp. 5-8.

[31] Algemeen Overleg met minister Van Boxtel d.d. 21 juni 2001, *Kamerstukken II*, 2000-2001, 25764, nr. 17.

[32] Zie de brief van minister Van Boxtel d.d. 11 mei 2001, *supra* noot 22.

[33] Algemeen Overleg met minister Van Boxtel *supra* noot 31, pp. 1-7.

[34] Ibid., pp. 4-9.

[35] '*Iedereen vingerafdruk laten afstaan*', Parool, 4 december 2001, p. 4 (cursivering VB).

[36] *Privacy*, Telegraaf, 5 december 2001, rubriek Kringen.

[37] Ibid.

[38] *Mondelinge test*, Volkskrant, 10 december 2001, p. 1.

[39] Ibid.

[40] Brief van de minister van Justitie (Benk Korthals) d.d. 10 december 2001, *Kamerstukken II*, 2001-2002, 19637 (Vluchtelingenbeleid), nr. 635, p. 7.

[41] Algemeen Overleg met minister Korthals d.d. 13 december 2001, *Kamerstukken II*, 2001-2002, 19637, nr. 642, pp. 3-4 (cursivering VB).

[42] Zie emails van Joop Wijn (werkzaam bij ABN AMRO) aan de auteur d.d. 28 januari en 10 februari 2010.

[43] WRR-interview Grijpink, *supra* noot 45, p. 3.

[44] Hierna aan te duiden als 'WRR-interview Knopjes'.

[45] Hierna aan te duiden als 'WRR-interview Grijpink'.

[46] Hierna aan te duiden als 'WRR-interview Van Troost'.

[47] Hierna aan te duiden als 'WRR-interview Provily & Van der Zanden'.

[48] Hierna aan te duiden als 'WRR-interview Van Munster'.

[49] Hierna aan te duiden als 'WRR-interview Delwel & Koedam'.

[50] Hierna aan te duiden als 'WRR-interview Ruifrok'.

[51] Hierna aan te duiden als 'WRR-interview Kooij & Levering'.

[52] Ibid., p. 5.

[53] WRR-interview Knopjes, *supra* noot 44, p. 7.

[54] Zie WRR-interview Grijpink, *supra* noot 45, p. 5; WRR-interview Knopjes, *supra* noot 44, p. 1; WRR-interview Van Munster, *supra* noot 48, p. 2. Grijpink en Knopjes zijn respectievelijk voorzitter en oud-voorzitter van het NBF. Wat de termen 'centrale' en 'decentrale' opslag van biometrie betreft dient de lezer zich overigens te realiseren dat hier 10 jaar geleden meestal iets anders mee bedoeld werd dan tegenwoordig (in Nederland) vaak het geval is. Vroeger verstond men onder 'decentrale opslag' over het algemeen opslag in de chip van het paspoort en onder 'centrale opslag' opslag in de gemeentelijke reisdocumentenadministratie. Tegenwoordig duidt de term 'centrale opslag' veelal op opslag in een nationale databank (die overigens ook uit meerdere gekoppelde databanken kan bestaan), terwijl 'decentrale opslag' vaak opslag bij de gemeente betreft. Uiteindelijk draait het dan ook (nog steeds) om de concrete techniek *achter* het abstracte (verschuivende) jargon.

[55] WRR-interview Van Munster, *supra* noot 48, p. 2.

[56] Ibid.

[57] WRR-interview Van Troost, *supra* noot 46, pp. 2-3.

2 HET BIOMETRISCHE PASPOORT ONDER DE KABINETTEN BALKENENDE I-IV

2.1 Naar *cruising altitude* op Europees niveau (2002-2004)

2.1.1 Nationale wetgevende haast

Op 1 oktober 2001 werd de Nieuwe Generatie Reisdocumenten (NGR) ingevoerd. Het beheer ervan kwam te liggen bij het agentschap BPR (Basisadministratie Persoonsgegevens en Reisdocumenten, ressorterend onder het ministerie van Binnenlandse Zaken, BZK) en de bestaande NGR-projectorganisatie werd afgebouwd. Medio 2002 berichtte de (inmiddels demissionaire) minister voor Grote Steden- en Integratiebeleid Van Boxtel de Tweede Kamer dat de lopende haalbaarheidsstudie naar biometrie in reisdocumenten (naast de nog lopende haalbaarheidsstudie naar elektronische identificatie)[1] eind 2002 zou worden afgerond en waarschijnlijk zou resulteren in een positief advies.[2] Deze haalbaarheidsstudie richtte zich primair op het effectief bestrijden van *look-alike* fraude. Een relevant wetsvoorstel ter wijziging van de Paspoortwet was echter reeds in april 2002 aan de Tweede Kamer voorgelegd; dit voorstel gaf een juridische basis aan de opname van een biometrisch kenmerk in het reisdocument.[3] (Zie over de parlementaire behandeling van dit wetsvoorstel par. 2.12 *infra*.).

2.1.2 Nederland neemt het Europese voortouw

Reeds in oktober 2001 had minister Van Boxtel een discussie over biometrie in reisdocumenten op Europees niveau geïnitieerd. Hiertoe had hij de voor reisdocumenten verantwoordelijke EU-ministers en de Europese Commissie geïnformeerd over de nieuwe Nederlandse reisdocumenten en het voornemen van de Nederlandse regering om in de nabije toekomst biometrie in reisdocumenten op te nemen. Ook had hij de wens uitgesproken om op het gebied van biometrie in reisdocumenten in Europees verband samen te werken. De reacties hierop waren positief, zowel van de lidstaten als van de Europese Commissie; de Europese Commissaris voor Binnenlandse Zaken en Justitie (JBZ) had het onderwerp tevens geagendeerd voor de JBZ-raad. Naar aanleiding van bilaterale gesprekken vanuit BZK werd vervolgens besloten om een Europese conferentie te organiseren teneinde informatie te kunnen uitwisselen en een basis te kunnen leggen voor Europese samenwerking. Deze conferentie vond in juni 2002 in Nederland plaats.[4] Naast de voor de uitgifte van reisdocumenten verantwoordelijke autoriteiten van de EU-lidstaten werd de conferentie onder andere bijgewoond door vertegenwoordigers van de Europese Commissie, ICAO, de Verenigde Staten en Canada. Veel interesse was er voor de Nederlandse NGR en de haalbaarheidsstudie naar de invoering van biometrie. Op dit laatste terrein liepen vier

Europese landen voorop: het Verenigd Koninkrijk, Duitsland, Italië en Nederland, allen met als primaire doelen om *look-alike* fraude terug te dringen, geautomatiseerde grenscontrole te faciliteren en/of het aanvraagproces beter te beveiligen.[5] Op voorstel van Nederland eindigde de conferentie met gezamenlijke besluiten om het belang van biometrie in reisdocumenten te onderschrijven, de discussie in ICAO over biometrie actief en in onderling overleg te voeren en een gezamenlijk forum (het *European Forum for Travel Documents*) op te richten waarin Duitsland, het Verenigd Koninkrijk, Italië, Frankrijk en Nederland als voortrekkers (*Standing Committee*) zouden fungeren. Dit Forum zou een rol gaan vervullen in informatie-uitwisseling en samenwerking binnen Europa op het terrein van (standaardisering en harmonisering) van biometrie in reisdocumenten. "Met dit resultaat heeft Nederland een belangrijke bijdrage geleverd aan de totstandkoming van een Europees standpunt op het gebied van biometrie in reisdocumenten. De weg naar politieke besluitvorming op EU-niveau is hiermee ingezet," aldus de minister.[6]

Tekstbox 2.1

De deelname van de Verenigde Staten (VS) aan de conferentie in juni 2002 kwam voort uit toenmalige Amerikaanse ontwikkelingen met betrekking tot de aanscherping van regels om toegang te krijgen tot de VS. Op grond van het Amerikaanse *Visa Waiver Program* (VWP) had de VS sinds 1986 aan diverse landen een visumvrijstelling verleend voor tijdelijk bezoek aan de VS. Veel Europese landen, waaronder Nederland, maakten sindsdien van deze regeling gebruik.[7] Naar aanleiding van de aanslagen op 11 september 2001 werd een groot aantal nieuwe wetten door het Amerikaanse *Congress* aangenomen, waaronder de *Enhanced Border Security and Visa Entry Reform Act* van mei 2002. Deze wet stelde als eis dat landen die nu op grond van het VWP bij bezoek aan de VS een visumvrijstelling hadden, met ingang van 26 oktober 2004 over een paspoort met biometrie moesten beschikken. De vertegenwoordiger van het *US Department of State* lichtte tijdens de conferentie van juni 2002 deze nieuwe Amerikaanse wetgeving toe. Hij gaf aan dat de VS qua te hanteren biometrisch kenmerk ICAO zou volgen. Overigens was er destijds nog geen besluit genomen om ook biometrische kenmerken op te nemen in het eigen Amerikaanse paspoort.[8] (Inmiddels bevat het Amerikaanse biometrische paspoort alleen een gelaatsscan.[9])

2.2 Het EFTD/IF4TD: 'What happens in the Forum, stays in the Forum'

2.2.1 Van Europese naar wereldwijde expansie

Het *European Forum for Travel Documents* (EFTD) werd in november 2002 in Londen opgericht op initiatief van het Nederlandse agentschap BPR. In de Nederlandse parlementaire geschiedenis wordt het EFTD slechts in enkele Kamerstukken genoemd.[10] Verder wordt in een onderzoeksrapport van BPR uit juni 2003 opgemerkt dat het EFTD "naar het zich nu laat

aanzien (...) een belangrijke rol [zal] vervullen in de verdere afstemming [rond biometrie] in Europees verband."[11] Een nationale en internationale zoektocht in de journalistieke database LexisNexis levert echter geen enkele *hit* op en ook op het internet is bijzonder weinig over het EFTD te vinden. Uit de schaarse internetbronnen blijkt onder meer dat het EFTD na drie jaar van geografische expansie in december 2005 in Bangkok werd omgedoopt tot *International Forum for Travel Documents* (IF4TD) en dat het aantal (louter gouvernementele) leden ervan wereldwijd gestaag is gegroeid. [12] Zo was er eind 2008 de uitbreiding met de Malediven:

> "... [T]he Maldives has signed an agreement to become a member of the IF4TD at Tokyo, Japan on 13th November 2008. The membership is open for the Travel Document / Identity Card Issuing Authorities. Hence the benefit of becoming a member is to have a global central platform for information sharing and to communicate with experts on Travel document Issues and to deliver updated information on conferences / events globally. (...) The Maldives will be the first country to be the Member of IF4TD among South Asia."[13]

Blijkens een presentatie van voormalig EFTD/IF4TD-voorzitter Sjef Broekhaar (destijds werkzaam voor BPR; tegenwoordig voor de International Organization for Migration, IOM) omvatte het IF4TD in september 2007 in totaal 47 landen, 52 uitgevende instanties en 171 *participants* (dit omvatte destijds nog geen internationale organisaties).[14] In december 2009 was dit aantal volgens de opvolgende (tweede) IF4TD-voorzitter Edmee Gosselink (eveneens BPR) opgelopen tot "54 deelnemende landen en ruim 150 participanten".[15] Hieronder vielen inmiddels ook internationale organisaties, waaronder de Verenigde Naties (VN) en het Rode Kruis.[16] Kosten voor de leden zijn er niet en de voornaamste plicht voor leden lijkt te bestaan uit het up-to-date houden van eigen informatie op een gezamenlijke, besloten website.[17] In een email aan de auteur werd verder meegedeeld dat "het Europese Forum [in 2005] een Internationaal Forum [is] geworden, daar ook internationaal behoefte was om onderling kennis en ervaring uit te [wisselen] over de aanvraag- en uitgifte van reisdocumenten. [Nederland] heeft tot nu toe het voorzitterschap en het algemene secretariaat voor haar rekening genomen en het onderhoud van de website van het IF4TD. De regionale vertegenwoordigers voeren secretariaatswerkzaamheden uit voor hun eigen regio."[18] Het IF4TD is opgedeeld in vier regio's: Europa, de Amerika's, Afrika en Azië-Pacific. Behalve een *Standing Committee* heeft het IF4TD ook een *Advisory Board*. Het *Standing Committee* heeft maximaal 9 leden en bestond in januari 2010 uit vertegenwoordigers van Nederland, Verenigd Koninkrijk, Verenigde Staten, Hong Kong en Japan.[19] De *Advisory Board* bestaat uit leden van "institutions that do not issue travel documents (...) but play an important role for travel documents, international aviation, migration, or border management," waaronder de Europese Unie (EU), IOM, ICAO en de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE).[20] Het *Standing Committee* (SC) kiest elke drie jaar een voorzitter.[21] "Tot nu toe zijn de heer Broekhaar en [vervolgens mw. Gosselink, tot 1 januari 2010] voorzitter van het IF4TD geweest. Binnen de Standing Commissie [*sic*] zijn er een aantal plaatsen vrij

gekomen door het vertrek van een aantal personen en er heeft [in januari 2010] nog geen definitieve besluitvorming plaatsgevonden in de SC over het nieuwe voorzitterschap."[22] Ook in augustus 2010 zou er nog geen duidelijkheid bestaan over het nieuwe voorzitterschap. "Duidelijk is [echter] wel dat Nederland niet langer voorzitter wil zijn", aldus een welingelichte bron.[23] Verder zou de (besloten) website van het IF4TD inmiddels worden overgedragen aan ICAO en daarom tijdelijk uit de lucht zijn.[24] Momenteel staat deze website nog geregistreerd bij agentschap BPR.[25]

2.2.2 Schimmigheid troef

Op een vraag van de auteur over alle EFTD/IF4TD-conferenties van de laatste jaren en eventueel beschikbare verslagen daarvan werd vanuit agentschap BPR slechts geantwoord dat "het Forum zichzelf in de afgelopen jaren op diverse conferenties [heeft] gepresenteerd. Er is geen sprake van formele verslaglegging."[26] De meegezonden documentatie stelt in dit verband het volgende:

> "The UK, Italy and Germany plan to host the first 3 meetings starting in November 2002. These will take place approximately every 3 months including one main conference every year. (...) Any country acting as host for a Forum will arrange a chairperson and note taker for the meeting. (...) The Forum's primary purpose is to encourage information exchange between European countries, about the use of biometrics and related technologies in travel documents. All members and observers will agree to respect the confidentiality of any information supplied at Forum meetings and will not disclose the item outside its own organisation without the express consent of the country supplying the information. No formal minutes will be taken of Forum meetings but the host country will lodge a list of discussion topics, together with any agreements and reports on the Forum web site."[27]

Een vraag van de auteur over eventueel in het kader van het Forum gesloten multilaterale of bilaterale verdragen danwel *Memoranda of Understanding* (MoU's) bleef onbeantwoord. Het antwoord op vragen over een eventuele rol van het Forum bij de ontwikkeling van het biometrische paspoort en de kwestie van decentrale of centrale opslag van biometrische gegevens luidde als volgt:

> "Het Forum heeft geen enkele formele status en ontplooit ook geen activiteiten in [het] kader van de ontwikkeling van het elektronisch paspoort anders dan het registreren / uitbreiden van de reeds bestaande informatievelden met relevante informatie. Het Forum is gericht op de uitvoerende instanties en niet op de beleidsmakers, het is statisch en heeft geen actieve discussiefunctie en ondersteunt dit technisch ook niet. Het wordt uitsluitend gebruikt om informatie te publiceren die overheden op het gebied van het aanvraag- en uitgifteproces van reisdocumenten willen delen. (...) [H]et Forum [is] geen platform waar besluitvorming wordt voorbereid of standpunten worden geïnventariseerd. De karakteristieken van het aanvraag- en uitgifteproces van de deelnemende landen worden in een landenprofiel geregistreerd. Het is aan het land zelf om informatie te verstrekken over de wijze waarop [het] nationale proces is ingericht."[28]

Niettemin viel in de eerdere parlementaire geschiedenis te lezen dat "een belangrijke rol in de ontwikkeling en vormgeving van de voorstellen aangaande biometrie in de paspoorten door

de Europese Commissie (...) naar verwachting vervuld [zou] worden door het European Forum for Travel Documents dat in 2002 op initiatief van Nederland is opgericht om op het gebied van reisdocumentenaangelegenheden samenwerking in Europees verband vorm te geven. (...) Nederland heeft [tijdens een bijeenkomst van het EFTD in november 2003 in Rome] het mandaat gekregen om namens de leden van het Forum nader overleg te voeren met de Europese Commissie over afstemming binnen Europa met betrekking tot biometrie in de reisdocumenten."[29] Dergelijke Europese afstemming (ook richting de Europese Raadsvoorzitter) blijkt eveneens uit een *unclassified* Amerikaans telegram uit juli 2003.[30] Dit telegram leert ons verder het volgende:

> "US policy concerning biometrics, machine readable passports (MRPs) and fingerprinting came under fire at the second European Forum for Travel Documents, which took place in Berlin June 30-July 1, 2003. (...) Participants (notably UK and Japan) were consistently and adamantly pessimistic about any country, including the US, meeting the US-set deadline of 26 October 2004 for production of passports with ICAO-standard biometrics. (...) Criticism of US policy emerged during initial discussions on common EU minimum security standards for travel documents, with the German delegates expressing concern that the dialogue in the EU was being driven by the demands of US legislation that was not clearly understood. There was also a strong undercurrent of resentment over having the terms and timetable of the debate set by US security concerns rather than common EU principles and decisions. (...) The British delegation (...) bluntly asserted that the US itself would be unable to meet its own deadline (...). Data security issues were not on the forum's formal agenda, but were very much on the mind of participants. Both the German and the Polish delegations expressed concern about the uses to which the US would put the fingerprint data to be collected from all travellers and visa applicants as of January 1, 2004. The US delegation stressed that the US had its own privacy and data protection laws that would apply to all data collected in connection with travellers – an assertion which caused several participants to shake their heads in disagreement. (...) The commitment of all participants to enhanced document security in the post-9/11 world is genuine, but it is difficult to deny the uneasiness with which the Europeans and Japanese view the strict new US requirements for VWP travelers. Our MRP and biometrics deadlines are seen as unrealistic and a major disruption to the right of travel; our use of data collected from travelers as suspect. (...) The overwhelming sentiment of most participants was clear: US policy and regulations were forcing European countries to move too quickly to adopt policies of questionable merit."[31]

Aan de andere kant lijkt de beschikbare informatie (waaronder ook enkele presentaties[32]) en genoemde correspondentie er op te duiden dat het EFTD/IF4TD 'slechts' een informeel netwerk of platform zou zijn ter onderlinge uitwisseling van informatie en expertise. De politieke gevoeligheden rondom de onderwerpen in kwestie zouden wellicht kunnen verklaren waarom een en ander zich structureel in strikte beslotenheid afspeelt. Het al dan niet legitieme karakter van die beslotenheid valt voor de objectieve buitenstaander echter onmogelijk te beoordelen zolang de betreffende onderwerpen onbekend blijven.

2.3 Ontwikkelingen op internationaal niveau

2.3.1 Biometrie in ICAO-verband en de Nederlandse keuze voor de gelaats- en vingerscan

Reeds sinds 1997 was ICAO bezig met onderzoek naar biometrische kenmerken met als doel een standaard daarvoor te ontwikkelen. Onderzoek werd verricht naar drie biometrische kenmerken: de vingerscan, gelaatsherkenning en irisscan. Op 28 mei 2003 had ICAO dit onderzoek afgerond met het besluit om gelaatsherkenning (c.q. de pasfoto) als standaard biometrisch kenmerk op te nemen in de ICAO-richtlijnen voor reisdocumenten.[33] Volgens minister voor Bestuurlijke Vernieuwing De Graaf (D66) was de voornaamste reden hiervoor gelegen in het feit dat de pasfoto voor reisdocumenten reeds internationaal gemeengoed was en dus gemakkelijk inpasbaar in de meeste uitgifteprocessen van de ICAO-lidstaten. Toepassing van andere kenmerken zoals de vingerscan en irisscan zou voor veel ICAO-lidstaten tot grote organisatorische en financiële gevolgen leiden.[34] In Nederland zou uit onderzoek van het ministerie van Binnenlandse Zaken inmiddels echter zijn gebleken dat gelaatsherkenning onvoldoende geschikt zou zijn om *look-alike* fraude te bestrijden[35] en dat de vingerscan hiervoor het meest geschikte biometrische middel zou zijn. De motivatie hiervoor was dat de technologie voor de vingerscan beter integreerbaar zou zijn in de bestaande processen en gebruiksvriendelijker zou zijn dan de irisscan. Bovendien was de iristechniek gepatenteerd waardoor er een afhankelijkheid zou ontstaan van één leverancier.[36] De minister concludeerde dan ook om, "[o]p grond van de uitkomsten van het onderzoek én van de besluiten in ICAO-verband (...) zowel een gelaatscan als een vingerscan in [het paspoort en de Nederlandse identiteitskaart] op te nemen. De gelaatscan waarborgt dat de Nederlandse reisdocumenten voldoen aan de internationale standaarden. De vingerscan maakt het mogelijk binnen Nederland, waar de Nederlandse reisdocumenten een centrale rol spelen in allerlei processen om de identiteit van personen te verifiëren, identiteitsfraude beter op te sporen."[37] Medio 2004 zou in dit kader (in samenwerking met een aantal gemeenten) een biometrische praktijkproef in het aanvraag- en uitgifteproces worden georganiseerd.[38]

2.4 Intermezzo: *insiders* aan het woord

In 2003 besloot ICAO dat contactloze chiptechnologie en gezichtsherkenning de standaard zou moeten gaan worden voor het internationale reisverkeer. "De Amerikanen wilden per se gezichtsherkenning in het paspoort, ingegeven door terrorismebestrijding," zo licht Ruud van Munster toe.[39] Het voornaamste argument voor de gezichtsscan was volgens Fons Knopjes dat dit "de minste impact had op reeds bestaande processen en dat men de gebruikers ervan er daarom goed op zou kunnen aansturen."[40] Eerder had Knopjes zich echter kritisch

uitgelaten over de invoering van het biometrische paspoort ter bestrijding van *look-alike* fraude:

> "Er zijn 16 miljoen Nederlanders. Laten er 10 miljoen een identiteitsdocument hebben. Lookalikefraude laat zich nog niet in een promillage uitdrukken. Moet je 10 miljoen mensen met een biometriepas opzadelen omdat je met duizend een probleem hebt? Puur het tegengaan van lookalikefraude lijkt me niet het juiste motief."[41]

Hier denkt Ron van Troost inmiddels echter heel anders over:

> "Overigens hoeft het hierbij niet per se om grote aantallen te gaan: het *gebeurt*, en wat mij betreft is *elk* geval van identiteitsfraude er één teveel. De identiteitsketen dient zo schoon mogelijk te worden gehouden en we moeten er *alles* aan doen om dat voor elkaar te krijgen. Het gaat daarbij immers ook om het vertrouwen in het publieke bestel."[42]

Tekstbox 2.2

Desgevraagd bleken exacte cijfers over identiteitsfraude (inclusief *look-alike* fraude) met Nederlandse reisdocumenten tijdens vrijwel alle interviews onbekend.[43]

Uit recente statistieken over identiteitsfraude van het Expertise Centrum Identiteitsfraude en Documenten (ECID) te Schiphol blijkt dat het aantal geconstateerde *look-alike* fraudes met Nederlandse paspoorten en ID-kaarten in 2009 in totaal 63 was.[44] Bovendien zou het hierbij niet om zware criminaliteit of terrorisme gaan, maar om fraude met sociaal-economische motieven (voornamelijk asielzoekers). Inclusief het aantal niet-gesignaleerde gevallen zou het totale aantal in 2009 naar schatting niet meer dan 130 bedragen.[45] Cijfers uit eerdere jaren zouden in dezelfde orde van grootte liggen, al zou het aantal gevallen van *look-alike* fraude in procentuele zin licht zijn toegenomen. De algemene trend zou echter al jaren zijn dat het absolute aantal gevallen van (alle vormen van) identiteitsfraude met Nederlandse paspoorten en ID-kaarten gestaag afneemt.[46]

Overigens blijkt het voor de Nederlandse overheid nog altijd moeilijk om een compleet, landelijk dekkend beeld te krijgen van identiteitsfraude met Nederlandse identiteitsdocumenten (inclusief paspoorten en ID-kaarten), zowel vanwege het ontbreken van binnen- en buitenlandse meldplichten terzake als vanwege gebrekkige samenwerking tussen relevante overheidsinstanties.[47]

Sinds '9/11' bewaren de Amerikanen vingerafdrukken in een databank.[48] Jan Grijpink is kritisch over de gevolgen die deze ontwikkeling voor Nederland heeft gehad:

> "De enige verstoring van het rationele proces is '9/11' geweest. Daarna zijn de Amerikanen biometrie van buitenlanders gaan verzamelen. (...) De Amerikaanse eisen werden eenzijdig

> opgelegd onder het *Visa Waiver Program*. Mijn idee was destijds: daar beginnen we toch niet aan? En als dat *Visa Waiver* programma dan niet voor Nederland of niet voor alle Nederlanders geldt: jammer dan. Ik zou destijds gekozen hebben voor *vrijwillige* opname van vingerafdrukken in het paspoort (...) voor mensen die naar Amerika willen reizen."[49]

De vingerafdruk (en/of irisscan) was (en is) overigens géén internationale ICAO-*eis*, maar slechts een ICAO-*aanbeveling* voor binnenlands gebruik.[50] Met name vanwege het feit dat op het terrein van irisscans voorheen sprake was van een monopolie, werd op Europees niveau (naast de gezichtsscan) vervolgens gekozen voor invoering van de vingerafdruk, aldus Knopjes.[51]

2.5 Tussenconclusie

Look-alike fraude met Nederlandse reisdocumenten blijkt in kwantitatieve zin al jaren een relatief kleinschalig fenomeen, wat dringende vragen oproept over de algehele proportionaliteit (en daarmee ook de *efficiëntie*) van het biometrische paspoort als middel ter bestrijding van dit type fraude. Naarmate de ontwikkeling van het biometrische paspoort het nationale niveau (verder) ontstegen is en op Europees en internationaal niveau terecht is gekomen, zijn twee andere beginselen eveneens op scherp gezet: *transparantie* en *accountability*. Dit geldt met name voor het EFTD/IF4TD, waarvan gesteld kan worden dat *alle* beginselen er vrijwel uit beeld zijn verdwenen, althans voor de buitenstaander c.q. de burger. Zo bezien bleef er op dit terrein van de relatie burger-overheid in wezen reeds sinds 2002 niet veel meer over. Van alle beginselen lijkt het sindsdien echter nog het slechtst te zijn gesteld met de *keuzevrijheid*, niet alleen voor de burger, maar ook voor de Nederlandse staat zelf: als lid van het Amerikaanse VWP werd het voor Nederland immers 'biometrie slikken of stikken'. Het latere gebrek aan biometrische keuzevrijheid voor de Nederlandse burger zou in die zin dus ook gezien kunnen worden als een indirecte, blijvende erfenis van de Amerikaanse regering Bush; een erfenis die de Nederlandse regering destijds aanvaard heeft en waar de Nederlandse bevolking sindsdien mee geconfronteerd wordt. Aan de andere kant was het destijds de Nederlandse overheid zélf die voor de gelaatsscan én vingerafdrukken koos; internationaal gezien had men het immers bij de gelaatsscan kunnen laten. (Al zou de opname van vingerafdrukken onder de latere Europese paspoortverordening alsnog verplicht worden.) Hieronder zal worden ingegaan op het Nederlandse overheidsonderzoek dat destijds de aanleiding zou hebben gegeven tot deze keuze.

2.6 Onderzoek van agentschap BPR naar de toepassing van biometrie in Nederlandse reisdocumenten (2003)

2.6.1 Overzicht van eerder BZK-onderzoek naar het gebruik van biometrie (1998-2003)

Begin juni 2003 verscheen in het kader van de sinds 1998 lopende haalbaarheidsstudie naar de invoering van biometrie in Nederlandse reisdocumenten een onderzoeksrapport van het agentschap BPR (BZK).[52] De voornaamste onderzoeksvraag in dit rapport betrof de geschiktheid van biometrie voor het bestrijden van *look-alike* fraude en de vraag welk biometrisch kenmerk daartoe de voorkeur verdiende.[53] Tevens was onderzocht hoe biometrie op de Nederlandse reisdocumenten in de tijd ingevoerd diende te worden. Hierbij waren ook de internationale ontwikkelingen terzake betrokken.[54] Het onderzoek beperkte zich tot drie biometrische kenmerken: gelaat, iris en vingerafdruk (dit sloot aan bij toenmalige ontwikkelingen in ICAO-verband). Verder lag de focus op biometrische 1:1 verificatie in fysieke aanwezigheid (in plaats van verificatie op afstand) van de houder van het document. “Voor vergelijking van het afgenomen biometrische kenmerk met in een database opgeslagen kenmerken [was] om redenen van privacybescherming niet gekozen.”[55] Dit onderzoeksrapport volgde op een reeks van eerdere bevindingen, namelijk:

1. het feit dat bij de start van het NGR-project werd “onderkend dat de toepassing van biometrie mogelijkheden [bood] om de beveiliging van reisdocumenten verder te verhogen”, waardoor ook ter bestrijding van *look-alike* fraude “een effectievere en meer betrouwbare verificatie van de identiteit [zou kunnen] plaatsvinden.”[56] Een ‘eerste verkenning’ in het kader van NGR in 1998 concludeerde vervolgens dat toepassing van biometrie in de (nieuwe generatie) reisdocumenten mogelijkheden bood en dat deze technologie zich snel ontwikkelde, maar in de praktijk nog nauwelijks grootschalig was beproefd. Ook ontbrak inzicht in de gevolgen van de invoering, met name op het gebied van privacy en maatschappelijke acceptatie.[57]
2. In 1999 had TNO in opdracht van BZK onderzoek gedaan naar de geschiktheid van biometrie ter bestrijding van *look-alike* fraude. Hieruit zou slechts zijn gebleken “dat enkele biometrische technieken (vinger, iris en gelaat) nader beschouwd [moesten] worden op bruikbaarheid in het toepassingsgebied dat [BZK] voor ogen [had]. Tevens [waren] enkele kritische succesfactoren aangegeven, waaronder de organisatie, de acceptatie door de gebruikers en de betrouwbaarheid van de technologie. Daarnaast [waren] aanbevelingen gedaan ter aanscherping van de beoordelingscriteria, geënt op een gedetailleerde beschrijving van de toepassingscriteria.”[58]
3. In 2001 werden in opdracht van de toenmalige minister voor Grote Steden- en Integratiebeleid enkele kleinschalige *pilots* uitgevoerd naar de praktische toepasbaarheid van biometrie en de acceptatie ervan bij het publiek. Uit een *pilot* in Rotterdam bleek dat

de "toenmalige stand van [irisscan]techniek nog niet volledig geschikt was voor de door BZK gewenste toepassing."[59] Daarnaast bleek dat de opname van biometrische kenmerken de nodige begeleiding van burgers vergde. Twee andere *pilots* met vingerscans (in Delft en Amsterdam Oud Zuid) waren gericht op "ondersteuning bij identificatie van elektronische transactie- en participatiediensten" en niet op biometrie ter bestrijding van *look-alike* fraude.[60]

4. Daarnaast was in 2001 in opdracht van de minister een onderzoek uitgevoerd naar de toegevoegde waarde van biometrie bij identiteitsvaststelling. Dit onderzoek bevestigde de geschiktheid van biometrie ter verbetering van identiteitscontrole aan de hand van reisdocumenten. "Daarmee [was] biometrie *in principe* een geschikt instrument ter bestrijding van *look alike* fraude."[61] Wel diende onder andere nog aandacht te worden besteed aan de vraag "in hoeverre de burger een belang heeft of waarneemt bij de toepassing van biometrie."[62]

Reeds begin 2002 bleek vervolgens "de bedoeling van het kabinet (...) om op korte termijn biometrische gegevens op te nemen in reisdocumenten ter bestrijding van *look alike* fraude."[63] Daarbij werden twee resterende vragen onderkend, namelijk 1) de vraag welke biometrische kenmerken zouden worden gebruikt en 2) de wijze van invoering ervan op de Nederlandse reisdocumenten. Deze vragen zouden uiteindelijk pas worden beantwoord in het onderzoeksrapport van juni 2003. Een relevant voorstel ter wijziging van de Paspoortwet werd echter reeds (zoals eerder al opgemerkt) in april 2002 ingediend.[64]

2.6.2 Biometrie op de agenda van interdepartementale stuur- en werkgroepen

In de inleiding van het onderzoeksrapport van juni 2003 wordt vermeld dat "de interdepartementale stuurgroep Fraude en Financieel-economische Criminaliteit ervan [uitgaat] dat het schadebedrag per valse identiteit circa € 36.000 bedraagt, vooral door belastingontduiking en frauduleus beroep op sociale voorzieningen. Deze stuurgroep heeft dan ook prioriteit gegeven aan identiteitsfraudebestrijding in de periode 2002-2008 en daarbij de introductie van biometrie als een belangrijke maatregel genoemd. Ook diverse ziektekostenverzekeraars hebben aangegeven dat het op correcte wijze identificeren van cliënten/patiënten een aanzienlijke besparing op de kosten van de zorg zou kunnen opleveren. De omvang van de schade wordt geschat op een bedrag van € 30 tot 40 miljoen per jaar. De Nederlandse Vereniging van Ziekenhuizen ziet de toepassing van biometrie als een belangrijk middel om deze schade te beperken."[65] Ook stelt de inleiding dat "*look alike* fraude een belangrijk aandeel vormt in de identiteitsfraude die met reisdocumenten wordt gepleegd."[66] Zo zou uit een onderzoek naar mensensmokkel in 2000 en 2001 zijn gebleken "dat het gebruik van valse en vervalste reis- en identiteitsdocumenten bij mensensmokkel

een hoge vlucht heeft genomen. *Look alike* fraude blijkt daarbij een belangrijke vorm te zijn. Tevens blijkt uit een [in 2002 door de Britse Immigratiedienst uitgevoerd onderzoek] dat *look alike* fraude ongeveer 78% uitmaakt van het totaal onderkende aantal fraudegevallen met Nederlandse reisdocumenten in het Verenigd Koninkrijk."[67] Ook de interdepartementale werkgroep terrorismebestrijding had aangegeven dat het van het grootste belang zou zijn om zekerheid te krijgen over de identiteit van reizigers. Zowel nationaal als internationaal zou daartoe geïnvesteerd worden in uitbreiding van de mogelijkheden van biometrie.[68]

2.6.3 Onderzoeksrapport BPR 2003: voornaamste passages en tussenconclusies

Het eerste deel van het onderzoeksrapport behandelt de biometrische techniek:

> "In de technische verkenning is de bruikbaarheid van biometrische techniek voor bestrijding van *look alike* fraude op Nederlandse reisdocumenten onderzocht. *Het onderzoek is uitgevoerd door bestudering van openbare literatuurbronnen.* In opdracht van het Agentschap BPR hebben VKA en TNO dit onderzoek verricht."[69]

Overigens viel het vergelijken van een 'live' afgenomen biometrisch kenmerk van een persoon met meerdere biometrische kenmerken van verschillende personen in een database (biometrische identificatie) buiten de reikwijdte van het onderzoek.[70] Verder bestond het technische deel van het onderzoek ook uit een marktverkenning door middel van informatieverzoeken aan relevante marktpartijen (uitgevoerd door Montelbaan in opdracht van BPR);[71] voor nadere beschouwing hiervan (alsmede van andere technische en industriële aspecten) wordt de lezer echter verwezen naar een parallel 'black box'-onderzoek van de WRR.[72] De andere delen van het onderzoeksrapport hadden betrekking op nationale en internationale afstemming, communicatie en draagvlak, beheer, procedures en infrastructuur, en financiën. Voorzover hier relevant worden de belangrijkste conclusies en opvallende passages uit het onderzoeksrapport weergegeven:

- Uit zowel de technische verkenning als de marktverkenning bleek dat irisherkenning de beste *performance* had, direct gevolgd door de vingerscan. De *performance* van gelaatsherkenning bleef aanzienlijk op deze twee kenmerken achter.[73]
- Uit de technische verkenning bleek echter tevens dat de vingerscan beter integreerbaar en gebruiksvriendelijker was. "De vingerscan [was daarom] momenteel het meest geschikte biometrische kenmerk voor de bestrijding van *look alike* fraude."[74]
- Hoewel in het reeds ingediende wetsvoorstel ter wijziging van de Paspoortwet[75] gekozen was voor opslag van biometrische kenmerken als *templates*, bleek uit de technische verkenning dat "als gevolg van voortschrijdende technische ontwikkelingen het niet uitgesloten kan worden dat uit templates bepaalde fysieke of persoonlijke kenmerken van de houder kunnen worden afgeleid. Hiermee is het argument om per se gebruik te maken van een template vervallen. (...) De toepassing van biometrie, in de vorm van (...) digitale

afbeeldingen, betekent niet dat er sprake hoeft te zijn van een onevenredige inbreuk op de persoonlijke levenssfeer van personen. In dit verband kan worden opgemerkt dat reis- en identiteitsdocumenten altijd al van afbeeldingen zijn voorzien waaruit fysieke of persoonlijke kenmerken kunnen worden gereconstrueerd, zoals de foto en de handtekening.”[76]

- De Interdepartementale stuurgroep Fraude en Financieel-economische Criminaliteit had aangegeven dat een ketenbrede aanpak noodzakelijk was om de veelheid aan (overheids)instanties die slachtoffer waren van identiteitsfraude gezamenlijk met behulp van de maatregel biometrie omvangrijke besparingen en betere efficiency te laten realiseren.[77]
- Ter voorbereiding van het gebruik van biometrie door verschillende overheidsinstanties werd overleg gevoerd met onder andere het ministerie van Sociale Zaken, het ministerie van Justitie, de Directie Politie van BZK, de afdelingen burgerzaken van gemeenten en de Koninklijke Marechaussee.[78]

2.6.4 Meting van maatschappelijk draagvlak

Het onderzoeksrapport van BPR vermeldt tevens dat door bureau Veldkamp kwantitatief en kwalitatief onderzoek (onder respectievelijk 1334 en 46 personen) was gedaan ter meting van het maatschappelijke draagvlak voor de invoering van biometrie in reisdocumenten. Uit dit onderzoek zou een relatief groot draagvlak zijn gebleken:

> “Volgens de respondenten zijn de twee grootste voordelen van de invoering van biometrie op reisdocumenten de bestrijding van *look alike* fraude en fraude door vervalsing van het reisdocument. Uit het kwalitatieve onderzoek blijkt dat de respondenten positief tegenover de opname van het biometrisch kenmerk staan omdat de eigen veiligheid erdoor wordt vergroot. (...) De percentueel meest genoemde nadelen hebben te maken met de inbreuk op de privacy die met de invoering van biometrie gemoeid zou zijn. Het lijkt er vooral om te gaan dat men vreest bij de invoering van biometrie geen controle te hebben over waar de biometrische gegevens terechtkomen en dat de overheid alles over de burgers te weten komt. De twee andere nadelen die het meest worden genoemd zijn meer praktisch van aard: controle op biometrische kenmerken zou tijdrovend zijn en hoge kosten met zich meebrengen.”[79]

Bijzonder opvallend zijn verder de volgende passages:

> “Uit het kwalitatief onderzoek blijkt dat de acceptatie van biometrische verificatie gekoppeld blijkt te zijn aan de situaties waarmee de respondenten zelf reeds ervaring hebben opgedaan. Voor situaties als bijvoorbeeld op het gemeentehuis of op Schiphol blijkt een breed draagvlak te bestaan. In deze context draagt biometrie bij aan de eigen veiligheid en aan de voorkoming van misbruik. Ten aanzien van de toepassing van biometrie bij alcoholcontrole en in het ziekenhuis is de weerstand wat groter. De sterkste weerstand bestaat ten aanzien [van] de controle van biometrische kenmerken door banken en daarnaast tegen *controle van biometrische kenmerken tijdens een demonstratie*. (...) Vrijwel alle respondenten vinden dat regels en wetten belangrijk zijn om burgers te beschermen tegen misbruik van hun gegevens door de overheid. Veel respondenten vinden bovendien dat de overheid te veel door regels beperkt wordt bij het opsporen van criminelen en dat het bestrijden van criminaliteit belangrijker is dan de bescherming van privacy.(...) *Uit het kwalitatief onderzoek komt naar*

> *voren dat de respondenten nogal eens denken dat er een koppeling zal plaatsvinden met een algemene database. Dit wordt niet uitsluitend als nadelig gezien, als positief gevolg wordt vermeld dat hiermee de identificatie en opsporing worden vergemakkelijkt.*"[80]

Een exacte (bron)vermelding, analyse en concrete cijfers van dit onderzoek ontbreken echter. Niettemin luidt de eindconclusie in het onderzoeksrapport van BPR dat "de grondhouding van de burger ten opzichte van biometrie overwegend positief te noemen is, waarbij het gevoel van toegenomen veiligheid een rol speelt."[81]

2.6.5 Eindconclusie onderzoeksrapport BPR 2003: verplichte invoering van RFID-chip met vinger- en gelaatsscan

De hoofdconclusie van het onderzoeksrapport luidt dat er moest worden gekozen voor een invoeringsscenario waarbij twee biometrische kenmerken in de chip van reisdocumenten zouden worden opgenomen: 1) een vingerscan ter bestrijding van *look-alike* fraude en 2) gelaatsherkenning voor internationale grenspassage.[82] Tenslotte werd in de enige bijlage van het rapport (over "alternatieve invoeringsscenario's") nog enige aandacht besteed aan eventuele keuzevrijheid voor de burger, en wel als volgt:

> "*Keuzevrijheid: al dan niet biometrie*
> In dit invoeringsscenario wordt de burger de keuze gegeven tussen een reisdocumenten [*sic*] met of zonder biometrie. Dit scenario is principieel onwenselijk. Het uitgangspunt, waarbij een uniform reisdocument voor de Nederlandse burgers beschikbaar is, dient te worden gehandhaafd. Daarnaast valt de bestrijding van *look alike* [fraude] middels biometrie natuurlijk niet te combineren met de keuzevrijheid van de burger. Tenslotte zou een document voorzien van biometrie, indien volledig te betalen door de burger die daarvoor kiest, extreem hoge kosten met zich meebrengen. In het andere geval zouden burgers die afwijzend staan tegenover de toepassing van biometrie, wel hieraan financieel moeten bijdragen.
>
> *Keuzevrijheid: al dan niet* ICAO *kenmerk*
> Dit invoeringsscenario gaat ervan uit dat de vingerscan in het reisdocument wordt opgenomen en dat de burger de mogelijkheid krijgt om al dan niet te kiezen voor het ICAO kenmerk, namelijk gelaatsherkenning. Alleen die burgers die naar een land reizen waar op basis van de ICAO-richtlijnen verificatie plaatsvindt kunnen dan dit kenmerk op hun reisdocument laten aanbrengen. Vanuit financieel oogpunt is dit geen aantrekkelijk scenario. Bij de toepassing van gelaatsherkenningtechnologie is weliswaar geen enrolmentapparatuur nodig, maar daar staat tegenover dat de logistiek van het productieproces bij de leverancier van de reisdocumenten ingewikkelder en dus ook duurder wordt."[83]

Op het bestaan van principieel bezwaarden of een eventueel scenario mét gelaatsherkenning maar zónder vingerscan werd in het geheel niet ingegaan. Aan een mogelijk scenario met een contactchip in plaats van een contactloze (op afstand uitleesbare RFID-)chip in het reisdocument werd in het onderzoek evenmin aandacht besteed. De keuze voor een contactloze chip leek immers voort te vloeien uit de relevante ICAO-richtlijnen in wording. Die ICAO-richtlijnen zouden echter 'slechts' gaan zien op verplichte gelaatsherkenning (in tegenstelling tot (tevens) een vingerscan) als minimaal te gebruiken biometrisch kenmerk voor reisdocumenten.[84]

2.7 Intermezzo: *insiders* aan het woord

2.7.1 Relevante TNO-rapporten

In opdracht van agentschap BPR had dhr. Ruud van Renesse (destijds TNO) in 1999 het rapport '*Quick scan biometrie – alle mensen zijn ongelijk*' geschreven; dit rapport verscheen op 29 oktober 1999.[85] Oud-collega Ruud van Munster vertelt hierover: "Het rapport werd door BPR gearchiveerd en pas later bekendgemaakt. (...) Het rapport was tamelijk kritisch over het gebruik van biometrie; dit echter ook in het licht van het feit dat de overheid nog geen heldere doelen voor biometrie had aangegeven. Het rapport ging over biometrie in het paspoort voor grenspassage, gebruik van biometrie in het gemeentehuis en thuisgebruik. (...) Zelf vond ik het rapport nog relatief mild, maar toch reageerde BPR als door een wesp gestoken."[86] Jaren later (in december 2002) verscheen het rapport '*Biometrics against look alike fraud in the next generation travel documents*' van VKA en TNO.[87] "Dit rapport is vervolgens ook veel gebruikt door andere organisaties, waaronder de IND en Montelbaan. Inmiddels was duidelijk dat biometrie in het paspoort primair bedoeld was om *look-alike* fraude te voorkomen. Het rapport was eigenlijk een grote literatuurstudie; er zijn zo'n duizend documenten voor geraadpleegd. (...) [Het] was eigenlijk vooral een *best practice* inventarisatie," aldus Van Munster.[88] Bij dit rapport was echter ook een laboratoriumproef (onder andere met tweelingen[89]) betrokken die TNO in juni 2002 had uitgevoerd en waaruit zou zijn gebleken dat "gezichtsherkenning leed onder de aanwezigheid van *look-alikes*: voor het herkennen van *look-alikes* bleek gezichtsherkenning, zoals verwacht werd, geen goede methode."[90] Het rapport van deze proef (daterend van september 2002)[91] heeft er volgens Van Munster destijds aan bijgedragen dat de vingerafdruk in het paspoort werd opgenomen.[92] De vraag of biometrie ook *in kwantitatieve zin* effectief zou zijn ter bestrijding van *look-alike* fraude zou echter nooit aan TNO zijn gesteld. Kwantitatieve gegevens over *look-alike* fraude zouden in de genoemde rapporten dan ook ontbreken.[93]

2.7.2 *Flash forward*: agentschap BPR

Uit de interviews bleek dat de Nederlandse ontwikkeling van het biometrische paspoort tot nu toe zou zijn gedomineerd door BZK (c.q. agentschap BPR), waar men zich vooral zou hebben gericht op de aanvraag- en uitgiftestructuur van de documenten.[94] "Bij een reorganisatie van BPR zijn beleid en uitvoering gesplitst. Het project 'biometrie in reisdocumenten' bevindt zich sindsdien fysiek nog bij BPR," vertelt Ron van Troost.[95] Beleidsmatig zou een en ander inmiddels onder een directie van BZK vallen. Uit veel interviews bleek dat de interdepartementale samenwerking met BPR veelal moeizaam was geweest, dat kritiek er niet werd gewaardeerd en dat amper sprake was (geweest) van externe

advisering. In dit verband zijn de volgende opmerkingen van (achtereenvolgens) Ruud van Munster, Peter Provily & Paul van der Zanden en Jan Grijpink karakteristiek:

> "... [A]ls TNO hadden we moeite om het 'bastion' BPR te bereiken. Zelf heb ik het altijd een lastig dossier gevonden, omdat we er als TNO wel de juiste expertise voor hadden maar opdrachten vaak gegund zagen aan partijen die zich meegaander opstelden. (...) Bij de concurrentie rond projecten van agentschap BPR werd voor TNO duidelijk dat de prijs voor BPR prevaleerde boven de kwaliteit. Hierbij speelde ook de gesloten cultuur van BPR een rol. (...) Agentschap BPR is één van de slechtst toegankelijke agentschappen van Nederland. Op het terrein van centrale opslag van biometrie is dat een zorgpunt. Een probleem met BPR is ook dat ze nauwelijks kennis delen met andere overheidsonderdelen."[96]

> "We hebben heel veel energie moeten steken in het tot stand brengen van de interdepartementale samenwerking.(...) We werken veel met andere departementen samen, en in veel gevallen verloopt *die* samenwerking gelukkig wél heel goed. In dit traject is het echter een zeer moeilijke wedstrijd geweest... Het waarom van die moeizame samenwerking is [ons] eerlijk gezegd ook nog steeds niet duidelijk."[97]

> "Een echte klankbordgroep of externe adviesgroep heeft BPR niet gehad. Zelf ben ik ook al jaren niet meer bij BPR geweest; ze vonden me te kritisch. Bij BPR houden ze niet van interne en externe kritiek, en dat is een eufemisme."[98]

2.8 Amerikaans-Europees biometrisch simultaanvliegen (2004-heden)

2.8.1 Nederlandse visumvrijstelling onder het Amerikaanse *Visa Waiver Program*

Met betrekking tot de ontwikkelingen vanuit de Verenigde Staten liet minister De Graaf de Tweede Kamer in december 2003 weten dat onder het Amerikaanse VWP met ingang van oktober 2004 uitsluitend landen vrijgesteld werden van de Amerikaanse visumplicht wanneer hun reisdocument was uitgerust met een biometrisch kenmerk dat voldeed aan de ICAO-richtlijnen óf wanneer die landen voorbereidingen troffen voor de invoering van biometrie op hun reisdocumenten. Nederland behoorde tot de landen die ingevolge het VWP reeds vrijgesteld waren van de visumplicht en zou naar verwachting op grond van het criterium "voorbereidingen treffen voor de invoering van biometrie" ook na oktober 2004 van die visumplicht vrijgesteld blijven.[99]

2.8.2 Ontwikkelingen richting de Europese paspoortverordening (2003 - 2004)

Op Europees niveau had de Europese Commissie in september 2003 reeds "twee verordeningenvoorstellen gedaan inzake de opname van biometrische kenmerken, zijnde het gelaat en twee vingers, op de visa en de verblijfsdocumenten voor onderdanen van zogenaamde derde landen. De Commissie [was] voornemens begin 2004 te komen met een voorstel op het gebied van paspoorten."[100] In november 2003 had Nederland tijdens een bijeenkomst van het EFTD (als hierboven reeds beschreven) het mandaat gekregen om namens de leden van dat Forum nader overleg te voeren met de Europese Commissie over afstemming binnen Europa met betrekking tot biometrie in reisdocumenten.[101]

Tekstbox 2.3

Ook op het niveau van de Raad van Europa vonden relevante activiteiten plaats. Zo kwam een juridische "group of specialists on identity and terrorism" in april 2004 (onder Nederlands voorzitterschap) onder andere tot de volgende aanbevelingen:

> "The creation or development of systems which allow identity checks with reference to civil status records and registers and population registers to be carried out rapidly (in particular *by means of a centralised system*) and in a reliable manner. (...)
>
> Give consideration to and promote research and ongoing cooperation between police scientists and institutions (...) in order to make greater use of scientific identification of individuals, especially through *the use of biometrics and DNA analysis, most notably in their use in identity documentation*."[102]

De eerder door de minister aangekondigde 'praktijkproef biometrie'[103] vond vanaf eind augustus 2004 in zes gemeenten[104] plaats. Deze proef diende ter voorbereiding van de invoering (eind 2006) van de gelaatsscan en een vingerscan op het paspoort en de Nederlandse identiteitskaart (NIK). De eerste resultaten van deze (vrijwillige) proef stemden de minister positief.[105] Ook in andere Europese landen vonden dergelijke proeven plaats. Tevens was er op Europees niveau door de Europese Commissie inmiddels een concept-verordening ingediend betreffende "normen voor de veiligheidskenmerken en biometrische gegevens in paspoorten van EU-burgers"; in april 2004 was de Tweede Kamer hierover geïnformeerd.[106] Deze verordening beoogde het paspoort van de EU-lidstaten veiliger te maken door geharmoniseerde minimum veiligheidsnormen voor te schrijven en door het gebruik van biometrische kenmerken verplicht te stellen. Naar verwachting zou de JBZ-raad van 25 en 26 oktober 2004 over de verordening beslissen.[107] Nederland was op dat moment (gedurende de tweede helft van 2004) EU-voorzitter.

2.8.3 Amerikaans-Europese JBZ-bijeenkomsten (september - oktober 2004)

Begin november 2004 informeerde de regering de Tweede Kamer naar aanleiding van twee (informele) JBZ-bijeenkomsten in EU-kader alsmede van twee JBZ-bijeenkomsten tussen de VS en de EU in het kader van gezamenlijke terrorismebestrijding. Thema's tijdens eerstgenoemde JBZ-bijeenkomsten (30 september en 1 oktober 2004 te Den Haag) waren onder andere:

1. internationale informatieuitwisseling in het kader van wetshandhaving ("in de toekomst mag het feit dat de informatie grensoverschrijdend is op zichzelf geen belemmering meer opleveren [voor uitwisseling]");
2. crisisbeheersing ("bij crisis met grensoverschrijdende aspecten dienen de inspanningen van lidstaten niet alleen het nationale belang, maar ook het belang van de andere lidstaten te dienen");

3. versterking van Europol / Eurojust ("Europol en Eurojust [krijgen] een centrale rol (...) bij bestrijding van grensoverschrijdende georganiseerde misdaad en terrorisme");
4. terrorismebestrijding ("in de toekomst dient het concept nationale veiligheid in de praktijk ook de veiligheid van de andere lidstaten te omvatten"); en
5. een gemeenschappelijk visumbeleid ("benadrukt [werd] dat biometrie een belangrijk aspect is, alsmede de interoperabiliteit van informatiesystemen").[108]

De JBZ-bijeenkomsten tussen de VS en de EU (18 en 30 september 2004 te Den Haag en Scheveningen) dienden ter implementatie van de afspraken die waren gemaakt tijdens de voorgaande EU-VS Top (26 juni 2004 te Dublin) over terrorismebestrijding. Hoofdthema's waren de uitwisseling van informatie en biometrie, bescherming van persoonsgegevens, beveiliging van transport en grensbewaking. Ook werd afgesproken dat de samenwerking tussen Europol en de VS zou worden geïntensiveerd en dat er een FBI *liaison officer* in Den Haag zou worden geplaatst.[109] Verdere details zijn niet openbaar gemaakt.[110]

2.8.4 Nederlandse aankondiging van centrale opslag van biometrie (januari 2005)

Begin 2005 leek in het kader van terrorismebestrijding een belangrijke kentering op te treden op meerdere beleidsterreinen. Een belangrijke kabinetsbrief in dit verband dateert van 24 januari 2005. Het eerste deel van deze brief schetst de context van dat moment:

> "Geconfronteerd met de dreiging van internationaal terrorisme, in het bijzonder islamistisch terrorisme, en de realiteit van islamitisch radicalisme binnen de eigen grenzen, heeft Nederland in korte tijd op een groot aantal terreinen systematisch maatregelen getroffen om in te spelen op de nieuwe situatie. Na de aanslagen in september 2001 werd een groot aantal uiteenlopende maatregelen getroffen gericht op bescherming en bewaking. In juni 2003 werd aanvullend een aantal wetswijzigingen en beleidsmaatregelen aangekondigd, gericht op het observeren en tijdig aanpakken van personen en organisaties die mogelijk betrokken zijn bij de voorbereiding van terroristische daden. In maart 2004 werden, mede in het licht van de aanslagen in Madrid, een heroriëntatie en intensivering van het beleid van politie en AIVD ingezet met betrekking tot de observatie van potentiële betrokkenen en het alerteringssysteem. In september 2004 werd begonnen met de inrichting van de Staf van de Nationaal Coördinator Terrorismebestrijding [NCTb]. Tevens werd een fundamentele uitbreiding van de strafvorderlijke bevoegdheden bij de bestrijding van terrorisme en een verdere uitbreiding van de capaciteit van de betrokken diensten in gang gezet. In november 2004 werd tenslotte, mede tegen de achtergrond van de moord op de heer Van Gogh, besloten tot een verdere versterking van de capaciteit van de AIVD en uitbreiding van de capaciteit op het terrein van bewaking en beveiliging. Deze versterking van het vermogen van de overheid om een antwoord te bieden op de dreiging van deze tijd is gepaard gegaan met een stroom nieuwe wetsvoorstellen, regelgeving, voorzieningen en beleidsmaatregelen. Sinds de aanvaarding van de nieuwe terrorismewetgeving zijn verdere wijzigingen van het wetboek van strafvordering en andere wetten die relevant zijn bij de bestrijding van terrorisme ingediend of in voorbereiding. *Dat alles is echter slechts het meest zichtbare deel van de voortdurend groeiende inspanning van de overheid bij de bestrijding van terrorisme en gewelddadig radicalisme.* Eerder is Uw Kamer aangekondigd dat bij wet geregeld wordt dat de minister van Justitie, in zijn hoedanigheid van coördinerend minister van terrorismebestrijding, in bedreigende situaties waar overleg of overeenstemming gezien de urgentie niet meer tot de mogelijkheden behoort, de doorslaggevende bevoegdheid heeft om de noodzakelijke maatregelen te treffen. Dat kan betekenen dat hij gebruikt [*sic*] maakt van bevoegdheden die liggen op het terrein van andere

> ministers. (...) *Voorts heeft Nederland de samenwerking met de VS (...) verder uitgebouwd en vastgelegd in diverse afspraken. Ook hier onttrekken de concrete resultaten zich evenwel veelal aan directe waarneming*, anders dan door het uitblijven van nieuwe gewelddadige aanslagen. Er is kortom veel aangepakt in de afgelopen jaren. Daar is overigens ook alle aanleiding voor. De dreiging is onveranderd ernstig. Nederland is niet gevrijwaard gebleven voor aanslagen, zoals duidelijk werd met de aanslag op de heer Van Gogh."[111]

In het kader van terrorismebestrijding werd in deze brief een groot aantal maatregelen opgesomd, waaronder ook (de reeds eerder, in andere beleidskaders geplande) activiteiten met betrekking tot biometrie. Zo werd melding gemaakt van de (inmiddels lopende) praktijkproef in 6 gemeenten waarbij biometrische proefreisdocumenten werden uitgegeven. Ook werd de verwachting uitgesproken dat de uitgifte van biometrische reisdocumenten in het najaar van 2006 zou kunnen starten.[112] Verder werd vermeld dat er "regelmatig overleg [zou komen] tussen de EU en de VS over bescherming van persoonsgegevens (...) en beveiliging van internet en biometrie."[113] Bijzonder opvallend was echter de volgende passage:

> "... [I]n het kader van terrorismebestrijding [zal], in aanvulling op het aanbrengen van biometrische kenmerken op visa en identiteitsdocumenten, een informatie-infrastructuur worden ontwikkeld, waarmee de mogelijkheid ontstaat om de identiteit tevens on-line te verifiëren. Dit veronderstelt dat de administraties van de identiteitsdocumenten met biometrische kenmerken *centraal zijn georganiseerd*. Aldus kan het groeiende aantal gevallen van de zogenaamde *look-alike*-fraude, waarvan ook terroristen gebruik kunnen maken, worden tegen gegaan. Voor de wijze waarop verificatie, via de infrastructuur, in de databases moet geschieden, zullen uitvoeringsprotocollen worden ontwikkeld. Een en ander vloeit voort uit het kabinetsstandpunt inzake de bestrijding van identiteitsfraude en de toezeggingen uit de Terugkeernota. De ontwikkeling van deze informatie-infrastructuur draagt bij aan de intensivering van de samenwerking op Europees terrein en levert een bijdrage aan de effectiviteit van de uitvoering van de identificatieplicht. Deze infrastructuur dient onder andere ter ondersteuning van de intensiveringen bij de uitvoerende diensten. De middelen die in deze brief worden gereserveerd hebben uitsluitend betrekking op de genoemde informatie-infrastructuur. Over een *centrale registratie van biometrische gegevens*, die ten grondslag ligt aan een informatie-infrastructuur, zal de minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties de Kamer op een later tijdstip nader informeren."[114]

Dit werd destijds algemeen opgevat als de eerste publiekelijke aankondiging van het kabinet Balkenende om tot centrale opslag van biometrische gegevens over te willen gaan,[115] oftewel, in de woorden van een Nederlandse *watchdog* op het terrein van de identificatieplicht, "een centrale database te willen bouwen."[116]

2.8.5 De Kamer nader geïnformeerd over centrale opslag van biometrie (april 2005)

Op 18 april 2005 ging minister voor Bestuurlijke Vernieuwing Pechtold (D66) (als eerder aangekondigd, nu echter tevens namens minister van Justitie Donner (CDA)) "in op de vorming van een centrale registratie van biometrische gegevens, die ten grondslag ligt aan een informatie-infrastructuur (...) inzake de bestrijding van terrorisme."[117] Met deze 'informatie-infrastructuur' zouden biometrische identiteitsdocumenten voortaan 'online'

kunnen worden geverifieerd in de administratie van die documenten. Het ging hierbij om de Nederlandse reisdocumenten en om vreemdelingendocumenten. Online verificatie werd noodzakelijk geacht "om (meer) zekerheid te kunnen krijgen omtrent de identiteit van de houder van het document en de betrouwbaarheid van het document. (...) In het kader van de bestrijding van terrorisme is het van het grootste belang dat voorkomen wordt dat terroristen de identiteit kunnen aannemen van andere personen en als gevolg daarvan onopgemerkt blijven. Daarnaast berokkent identiteitsfraude de samenleving in vele sectoren jaarlijks enkele miljoenen Euro's aan financiële schade."[118] De minister berichtte verder als volgt:

> "In de brief van 24 januari 2005 inzake de bestrijding van terrorisme is aangegeven dat de online verificatie veronderstelt dat de administraties van de identiteitsdocumenten met biometrische kenmerken centraal zijn georganiseerd. Voor de vreemdelingendocumenten is dat reeds het geval. De reisdocumentenadministratie evenwel kent thans een decentrale opzet inhoudende dat de administratie zich bevindt bij de instanties die reisdocumenten uitgeven. Dat zijn de gemeenten, de Nederlandse ambassades en beroepsconsulaten in het buitenland, de Kabinetten van de Gouverneurs in de Nederlandse Antillen en Aruba, de gezaghebbers van de eilandgebieden in de Nederlandse Antillen en de daartoe aangewezen brigades van de Koninklijke Marechaussee. Het voornemen was, zoals dat blijkt uit het wetsvoorstel uit 2002, om bij de invoering van biometrische gegevens in de Nederlandse reisdocumenten die gegevens ook op te nemen in de decentrale reisdocumentenadministratie. Gelet op de maatregelen die het kabinet noodzakelijk acht in het kader van de bestrijding van terrorisme en identiteitsfraude ben ik van plan het zuiver decentrale karakter van de reisdocumentenadministratie te wijzigen en tot centralisatie van de administratie over te gaan. Dit zal in een separaat wetsvoorstel worden geregeld dat mede gebaseerd zal zijn op het beleidskader voor de bestrijding van identiteitsfraude waar de minister van Justitie thans aan werkt. Het wetsvoorstel zal naast de opzet van de administratie, ook de bescherming en de beveiliging van de administratie regelen, alsmede welke instanties toegang zullen krijgen tot deze administratie."[119]

Tekstbox 2.4

In april 2006 uitte de Commissie Meijers "vooruitlopend op dit wetsvoorstel, haar bezwaren tegen de voorgenomen centrale administratie van biometrische gegevens (...). Een centrale administratie van biometrische gegevens houdt onmiskenbaar risico's van misbruik en onjuist gebruik in. Op deze risico's is door vele deskundigen en nationale en internationale data protectie autoriteiten gewezen (...). Zo is aangetoond dat het gebruik van biometrische data voor persoonsherkenning nog steeds niet onfeilbaar is. Identificatie of verificatie op basis van deze gegevens zal dus altijd een foutmarge inhouden. Centrale opslag van biometrische gegevens vergemakkelijkt de koppeling en gegevensuitwisseling met andere (Europese) bestanden. (...) Hierdoor wordt de controle die een individu kan uitoefenen op het gebruik van diens persoonsgegevens bemoeilijkt of zelfs onmogelijk gemaakt. Bovendien wijkt de bewindsman af van het algemene principe dat in Nederland personenadministraties van de overheid in beginsel decentraal worden opgezet (...). Het is de vraag of een dergelijke centrale registratie effectief zal zijn in het kader van terrorismebestrijding. (...) Bovendien is het de vraag of de voorgestelde systemen niet een dermate grote hoeveelheid informatie zullen opleveren dat deze door politieautoriteiten niet of nauwelijks nog is te verwerken."[120]

In een latere reactie hierop stelde de opvolgende minister voor Bestuurlijke Vernieuwing Nicolaï (VVD) het echter "prematuur [te vinden] van deze commissie om nu reeds, zonder de inhoud van het wetsvoorstel te kennen, uitspraken te doen over het gebrek aan onderbouwing en de miskenning van de mogelijke risico's."[121]

2.8.6 De Europese paspoortverordening en gefaseerde invoering van biometrie

In de brief van april 2005 informeerde minister Pechtold de Kamer tevens over de in december 2004 uitgevaardigde Europese verordening "betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten."[122] Doel van deze paspoortverordening was om de paspoorten en overige reisdocumenten van de lidstaten van de Europese Unie beter te beveiligen tegen vervalsing en frauduleus gebruik. Hiertoe schreef de verordening voor dat in deze documenten een opslagmedium (chip) zou worden gebruikt waarin zowel een gezichtsopname (de gelaatsscan) als twee vingerafdrukken zouden worden opgenomen. Onder de Europese verordening (en de bijbehorende, van ICAO afkomstige technische specificaties in een beschikking van de Europese Commissie) diende de chip met de gelaatsscan uiterlijk op 28 augustus 2006 te zijn ingevoerd. De invoeringstermijn voor de vingerafdrukken zou pas later in werking treden, namelijk zodra ook daar de technische specificaties voor waren vastgesteld door de Europese Commissie. Om deze reden besloot de minister om over te gaan tot gefaseerde (in plaats van gelijktijdige) invoering van gelaatsscan en vingerafdrukken in de Nederlandse reisdocumenten.[123] De bestaande Paspoortwet behoefde op dit terrein niet te worden gewijzigd aangezien deze niet strijdig was met de (rechtstreeks werkende) Europese verordening.[124]

Tenslotte liet de minister de Kamer weten dat de praktijkproef (in zes gemeenten) met biometrische test-reisdocumenten[125] "goed was verlopen". Deze proef (genaamd "2b or not 2b") liep van eind augustus 2004 tot eind februari 2005 en werd nog geëvalueerd. Van de (vrijwillige) deelnemers waren twee vingerafdrukken en een gelaatsscan opgenomen. In totaal waren bijna 15.000 biometrische testdocumenten geproduceerd.[126]

2.9 Biometrieproef *2b or not 2b* (2004-2005)

2.9.1 Gemeenteproef, kinderproef en Schipholproef

Over de praktijkproef met biometrische test-reisdocumenten verscheen in september 2005 het 'Evaluatierapport Biometrieproef 2b or not 2b' van BZK. Doel van de praktijkproef was geweest om 1) na te gaan hoe het aanvraag- en uitgifteproces ingericht moest worden

wanneer er biometrische kenmerken werden opgenomen en 2) te toetsen of de biometrische kenmerken (gelaatsscan en vingerscan) in de reisdocumenten geverifieerd konden worden.[127] Deelnemers aan de proef in zes gemeenten[128] ('gemeenteproef') waren door middel van een brief en een folder[129] geworven onder burgers die een nieuw regulier reisdocument zouden gaan aanvragen (in verband met het verlopen van hun bestaande document). Deelname aan de proef was geheel vrijwillig en leverde bovendien een korting van € 10,- op bij de aanvraag van het nieuwe reguliere reisdocument.[130] Conform de Wbp hadden de deelnemers toestemming gegeven voor het gebruik van hun persoonsgegevens en biometrische kenmerken in het kader van de proef; hierover had BZK vooraf overleg gevoerd met het CBP.[131] Naast de gemeenteproef was door TNO tevens een 'kinderproef' gedaan "om na te gaan of het mogelijk [zou zijn] om bij kinderen tot 14 jaar een gelaatscan te maken en vingerafdrukken op te nemen."[132] Ook was er nog een aparte 'Schipholproef' om de robuustheid van test-reisdocumenten (bij veelvuldig gebruik) te onderzoeken.[133]

Uitkomsten van de gemeenteproef en de Schipholproef

Uit het evaluatierapport blijkt over de proef in de gemeenten en op Schiphol onder meer het volgende:

- de opname van de gelaatsscan leek volgens Tabel 1 van het rapport in 100% van de gevallen te zijn gelukt; hierbij waren echter niet de gevallen meegerekend waarbij de opname van de gelaatsscan niet lukte (!).[134] Op twee andere plekken in het rapport blijkt dat het maken van een gelaatsscan in 98,4% van de gevallen lukte; de daaropvolgende verificatie van gelaatsscans lukte bij 97,8%.[135] Uitgesplitst naar verificatie van een gelaatsscan van een (door de burger meegebrachte) pasfoto (in plaats van een 'livescan' bij de gemeente zelf) is deze *success rate* vervolgens nog maar 95,8%;[136]
- de opname van beide vingerafdrukken lukte in 96,8% van de gevallen; de daaropvolgende verificatie daarvan lukte bij 92,8%;[137]
- de populatie van de gemeenteproef kende een oververtegenwoordiging van deelnemers in de leeftijd tussen 50 en 80 jaar;[138]
- de gemeenteproef bood geen uitsluitsel over de invloed van verschillende huidtinten op de verificatie; daarvoor was het aantal deelnemers aan de proef met verschillende huidtinten (1% donker en 7% getint) te gering;[139]
- uit de Schipholproef bleek dat minstens 83% van de testdocumenten (haar)scheurtjes was gaan vertonen;[140]
- in de conclusies van het rapport komen de slagingspercentages van de opname en verificatie van vingerafdrukken in het geheel niet terug.[141]

Verder bleek dat "de gemeenteambtenaren die de training bij de producent hebben gevolgd (...) niet altijd de opgedane kennis aan hun collega's hebben doorgegeven, onder andere vanwege tijdsdruk. Als gevolg daarvan is het voorgekomen dat ambtenaren onvoorbereid aanvragen en uitgiften van biometrische testdocumenten hebben afgehandeld. Verder is gebleken dat het schriftelijk verstrekte opleidingsmateriaal (zowel het opleidingsmateriaal dat voorafgaande aan de proef is uitgereikt als het aanvullende opleidingsmateriaal dat is verstrekt om het opnemen van de vingerafdrukken te verbeteren) op een enkele uitzondering na, gedurende de proef niet als naslagwerk is gebruikt."[142]

Uitkomsten van de kinderproef

Over de 'kinderproef' noteert het evaluatierapport onder meer het volgende:

> "TNO komt op basis van het in opdracht van het ministerie van BZK uitgevoerde onderzoek tot de conclusie dat het opnemen van vingerafdrukken bij kinderen jonger dan 4 jaar nagenoeg onmogelijk is. Als het al lukt om bij kinderen van 3 en 4 één vingerafdruk op te nemen, dan is dat veelal de duim. Vermoedelijk komt dit doordat de duim een groter oppervlak heeft dan de andere vingers. Bij het opnemen van vingerafdrukken is verder het volgende geconstateerd:
>
> - Baby's (jonger dan 8-9 maanden) kunnen een stevige vuist maken die erg lastig geopend kan worden. Dit kan het opnemen van vingerafdrukken aanzienlijk bemoeilijken omdat de vinger niet goed op de sensor is te plaatsen. Een vergelijkbaar situatie kan zich overigens voordoen bij personen met spastische verkrampingen van de handen;
> - Bij kinderen die veel duimzuigen is de huid van de vinger (erg) week. Van dergelijke vingers is het vaak niet mogelijk om een goede afdruk op te nemen. (...)
>
> Het maken van een live opname van het gezicht bij kinderen lukt in de meeste gevallen. Waar het niet lukt wordt dit veroorzaakt doordat de kinderen huilen of heel beweeglijk zijn waardoor het niet lukt om het kind lang genoeg recht in de camera te laten kijken. Een andere oorzaak is dat kinderen, als de gebruikte camara [*sic*] een relatief lange sluitertijd heeft, niet stil kunnen blijven zitten waardoor een onscherpe en daardoor onbruikbare opname ontstaat."[143]

2.9.2 Conclusies van de minister

In zijn brief aan de Kamer over de (belangrijkste) resultaten van de biometrieproef concludeerde de minister onder andere "dat het maken van een gezichtsopname conform de door de Europese Unie gestelde eisen mogelijk is. (...) Hoewel het bij 98,4% van de deelnemers aan de proef gelukt is om een gezichtsopname te maken, is vast komen te staan dat het nodig is om de eisen voor de foto die de burger moet inleveren (bij het aanvragen van een reisdocument) te verscherpen. Dit is nodig om de kans op een succesvolle verificatie bij controle te vergroten."[144] Over de vingerafdrukken deelde de minister mee dat "[h]et opnemen van kwalitatief goede vingerafdrukken complex [is], zowel voor de ambtenaren van de uitgevende instanties als voor de burger. De proef heeft naar mijn mening op dit punt een aantal belangrijke resultaten opgeleverd. De kwaliteit van de vingerafdruk is cruciaal. Is de opgenomen vingerafdruk van onvoldoende kwaliteit dan is de kans groot dat verificatie van de vingerafdruk bij controle mislukt."[145] Evenals in de conclusies van het evaluatierapport zelf werden in dit verband door de minister geen concrete getallen of percentages genoemd.

Verder was de minister “gebleken dat het opnemen van vingerafdrukken bij kleine kinderen moeilijk is. Bij kinderen tot 6 jaar is het bijna onmogelijk.”[146] Over de biometrieproef en het evaluatierapport zijn vervolgens geen Kamervragen gesteld.[147]

2.10 Intermezzo: *insiders* aan het woord

Als drijvende internationale krachten achter het biometrische paspoort werden door vrijwel alle geïnterviewden vier actoren genoemd: de Verenigde Staten (c.q. het *Visa Waiver Program*, VWP) en ICAO na ‘9/11’, de EU vanaf (de aanslagen in) 2004 en de industriële lobby reeds sinds eind jaren 90. “Nederland liep destijds vooruit op de VS; een en ander was door Nederland immers al in gang gezet vóór ‘9/11’”, zo merkt Ruud van Munster op.[148] Jan Grijpink stelt in dit verband het volgende:

> “Dezelfde mensen waar deze *drive* eind jaren 90 al vandaan kwam hebben waarschijnlijk geprobeerd om het vervolgens alsnog via Brussel voor elkaar te krijgen. (...) Eind 2004 was Nederland EU-voorzitter. Mijn vermoeden is dat Nederland toen voor de EU het vastleggen van vingerafdrukken Europees (3e pijler) heeft ingestoken.”[149]

De *push* vanuit de biometrische industrie kan voor de overheid (vooral in kleine landen) grote risico’s met zich meebrengen. Fons Knopjes stelt hierover het volgende:

> “De voornaamste *drive* voor invoering van biometrische paspoorten kwam en komt vanuit de VS en is sinds ‘9/11’ in een stroomversnelling geraakt. (...) Een belangrijk *issue* in het hele proces is de *drive* van de industrie om dingen erdoor te krijgen. Dat is misschien wel het allerbelangrijkste risico. De industrie heeft ontdekt dat identiteitsmanagement op de agenda staat bij overheden en anticipeert daar handig op. Omdat kennis en inzichten bij industrie en overheden niet op hetzelfde niveau zitten ontstaan risico’s die vaak resulteren in oplossingen die niet aansluiten op de behoeften of problemen van overheden. De industrie gebruikt deze onbalans in kennis om zo haar producten af te kunnen zetten. Er is een klein aantal biometrie-leveranciers met grote belangen, waaronder Motorola, NEC, Sagem en Cogent. Op het terrein van biometrie zijn er wereldwijd 4 à 5 grote spelers die biometrie-databases leveren; meer is het niet. Die domineren de business. Ze kunnen alles. De biometrische industrie heeft Bush na ‘9/11’ de invoering van een biometrisch paspoort geadviseerd. De industriële lobby is dé *driver* in het hele proces. En de tegenhanger daarvan, de overheid, is vaak niet in een gelijkwaardige positie met de industrie om over deze business te spreken. De leveranciers lopen als het ware gewoon over de overheid heen.”[150]

Dit wordt volgens Knopjes nog eens versterkt door “de gebrekkige deskundigheid bij politici. Men heeft nauwelijks enig idee wat dit dossier inhoudt. Ik heb als toehoorder zelf verschillende malen in de Kamer gezeten als dit soort zaken aan de orde waren. Nou, je bent verbaasd hoe oppervlakkig men uiteindelijk hiermee omgaat, terwijl de impact van dit soort ontwikkelingen voor onze maatschappij enorm is.”[151]

Gevraagd naar de biometrieproef *2b or not 2b* klonk er met name kritiek vanuit het Nederlands Forensisch Instituut (NFI). Volgens NFI-medewerker Arnout Ruifrok “werd het NFI pas bij ‘2b or not 2b’ betrokken toen alles rond die proef al afgesproken en vastgelegd

was."[152] Uit de data die de proef had gegenereerd kon vervolgens niet altijd goed worden opgemaakt "wat ze nou eigenlijk gedaan hadden".[153] Zo kon uit de proefresultaten met vingerafdrukken "geen chocola gemaakt worden."[154] Die "analyse achteraf van onvolledige en deels onbetrouwbare resultaten is natuurlijk nooit een goede zaak," aldus Ruifrok.[155]

2.11 Tussenconclusie

De ontwikkeling van het biometrische paspoort lijkt te zijn gedomineerd door BZK c.q. agentschap BPR, waarbij vanuit laatstgenoemd agentschap structureel sprake zou zijn geweest van een gebrek aan goede interdepartementale samenwerking, informatie-uitwisseling en omgang met kritiek (althans volgens externe ervaringsdeskundigen). Ook in het publieke domein valt een gebrek aan *transparantie* en *accountability* van de zijde van BZK/BPR op: zo werden in het BPR-onderzoeksrapport uit 2003 diverse eerdere studies rond het biometrische paspoort op relatief positieve wijze aangehaald, zonder dat de betreffende studies ooit openbaar waren gemaakt. Voor de burger viel (en valt) dan ook onmogelijk na te gaan hoe de conclusies en interpretaties van BPR zich verhielden tot het oorspronkelijke onderzoeksmateriaal. Ditzelfde gold voor het belangwekkende rapport '2b or not 2b' uit 2005: ook hier viel (en valt) amper zicht te krijgen op de oorspronkelijke, authentieke onderzoeksresultaten (die bovendien deels onbetrouwbaar zouden zijn). In dit rapport leek zelfs met enkele getallen te zijn gegoocheld en leken belangrijke onderzoeksresultaten te zijn verdoezeld en uit de conclusies van het rapport te zijn weggelaten. Bij nauwkeurige (in tegenstelling tot vluchtige) lezing maakt dit rapport dan ook een enigszins misleidende indruk. Wetenschappelijk verontrustend is tevens het feit dat het gebruik van biometrie ter bestrijding van *look-alike* fraude nauwelijks feitelijk (in tegenstelling tot theoretisch) lijkt te zijn onderzocht; dit terwijl dat voorheen nu juist de voornaamste onderzoeksvraag betrof en de bestrijding van *look-alike* fraude stelselmatig werd (en wordt) genoemd als de voornaamste reden voor de invoering van biometrie in reisdocumenten. De focus in de onderzoeken lag vooral op 1:1 verificatie van (test)reisdocumenten (van veelal blanke, vrijwillige testpersonen) en bestudering van bestaande literatuur. Van daadwerkelijk empirisch, realistisch eigen onderzoek naar de effectiviteit van biometrie ter bestrijding van *look-alike* fraude lijkt in het geheel geen sprake te zijn geweest. Een en ander kan wellicht verklaard worden door het feit dat de Nederlandse regering begin 2002 al kenbaar had gemaakt biometrie in reisdocumenten te willen opnemen 'ter bestrijding van *look-alike* fraude' en dat een relevant wetsvoorstel ter wijziging van de Paspoortwet reeds in diezelfde periode was ingediend. Vervolgens was het (vanuit overheidsperspectief) dus niet meer de vraag óf biometrie in reisdocumenten zou worden ingevoerd, maar nog slechts *hoe*. De onderzoeksrapporten uit 2003 en 2005 kunnen waarschijnlijk het beste in dat licht worden gezien en begrepen. Dit is vooral goed zichtbaar in het (eveneens ongepubliceerde)

deelonderzoek naar *maatschappelijk draagvlak*, waaruit resultaten zouden zijn voortgekomen die grotendeels parallel liepen met eerdere (maar ook latere) overheidsargumenten voor de invoering van biometrie. Een bijzonder opvallende passage in deze 'onderzoeksresultaten' is overigens de bevinding dat er onder burgers veel weerstand zou bestaan tegen controle van biometrische kenmerken tijdens openbare demonstraties. Dit potentiële (neven)doel van de invoering van biometrie in reisdocumenten wordt elders in de parlementaire geschiedenis totaal niet genoemd. Een andere opvallende passage betreft de observatie dat burgers zich zouden hebben afgevraagd of een en ander aan een algemene (centrale?) database zou worden gekoppeld. Diezelfde burgers zouden vervolgens hebben onderkend dat identificatie en strafrechtelijke opsporing hierdoor zouden worden bevorderd. Als gezegd is dit deelonderzoek echter nooit gepubliceerd; de resultaten ervan zoals die worden beschreven in het onderzoeksrapport uit 2003 zijn vooralsnog dan ook niet te controleren. Dit geldt ook voor de hoofdconclusie dat de burger overwegend positief zou staan tegenover de invoering van biometrie in reisdocumenten.

Naast deze problematiek inzake transparantie en *accountability* op nationaal niveau, speelt een en ander ook op internationaal niveau: voor de gemiddelde burger was en is op het terrein van biometrie volstrekt onduidelijk wat zich precies afspeelt op het niveau van ICAO (en de industriële lobby daaromheen), de EU (met name ook in EFTD-verband) en de Raad van Europa, alsmede tussen de VS, de EU en Nederland onderling, laat staan dat de burger zijn of haar eigen overheid (of andere overheden) hierop kan (laten) aanspreken.

Aan *keuzevrijheid* werd in het rapport '2b or not 2b' uit 2005 in het geheel geen aandacht besteed. (Behalve wellicht onbedoeld en impliciet in de zin van 'gestuurde vrijwilligheid', aangezien burgers *vrijwillig* aan deze proef konden deelnemen en hier zelfs *financieel voordeel* bij hadden.) Het onderzoeksrapport uit 2003 noemde de keuze voor de burger tussen wel of geen biometrie in het reisdocument "principieel onwenselijk" en besteedde in de summiere argumentatie hierbij geen aandacht aan de problematiek van principieel (gewetens)bezwaarden, noch aan een eventuele keuze voor de burger om wel of geen vingerafdrukken (naast de 'ICAO-verplichte' gelaatsscan) in het reisdocument te laten opnemen. In wezen werd hierdoor ook de *identiteit* van principieel bezwaarden en burgers die vrij over hun eigen lichaamskenmerken willen kunnen beschikken ontkend. Zo bleef het beginsel identiteit nog steeds beperkt tot haar meest schrale betekenis: die van het biometrisch identificeerbare (en opspoorbare), 'genummerde' individu. Verder speelde het beginsel keuzevrijheid (als ook in de vorige tussenconclusie al opgemerkt) hier niet alleen op individueel niveau, maar ook (en nog steeds, inmiddels sterker) op internationaal niveau: gezien de eisen van de VS onder het VWP, de richtlijnen van ICAO en de Europese

paspoortverordening bestond er voor Nederland op dit terrein in zekere zin allang geen keuzevrijheid meer, en daarmee indirect evenmin voor de Nederlandse burger.

Wat het beginsel *privacy* betreft viel in het onderzoeksrapport uit 2003 allereerst op dat "om redenen van privacybescherming" bewust was afgezien van biometrische identificatie door middel van opslag van biometrische gegevens in een database. De nadruk in het onderzoek lag op biometrische 1:1 verificatie in aanwezigheid van de fysieke persoon zelf.
Begin 2005 (na een serie bijeenkomsten tussen de VS en de EU) kondigde de Nederlandse regering echter aan te zullen overgaan tot centrale opslag van biometrische gegevens. Met deze belangrijke beleidskentering leek tevens een belangrijke kentering op te treden in het belang dat aan privacy werd gehecht: vanaf dit moment leek privacy meer en meer ondergeschikt te worden gemaakt aan belangen van veiligheid en terrorismebestrijding.

De drijvende internationale krachten achter de ontwikkeling van het biometrische paspoort zijn met name de VS (VWP), ICAO, de EU en de biometrische industrie geweest. In het algemeen kan deze industrie een dusdanig sterke kracht vormen dat dit risico's voor de overheid met zich mee kan brengen wegens onderlinge verschillen in belangen, veronderstelde problemen en behoeften. Gebrek aan kennis en inzicht bij de overheid (vooral bij politici) kan vervolgens leiden tot het leveren van onnodige 'oplossingen' door de industrie aan diezelfde overheid. Wat de beginselen *effectiviteit* en *efficiëntie* betreft viel in dit verband allereerst op dat reeds in 1998 was gesteld dat de toepassing van biometrie mogelijkheden zou bieden om de beveiliging van reisdocumenten te verhogen. Men ging er vanuit dat hierdoor een meer effectieve, betrouwbare verificatie van iemands identiteit zou kunnen plaatsvinden en dat daardoor ook *look-alike* fraude beter bestreden zou kunnen worden. Destijds werd echter tevens onderkend dat biometrie in de praktijk nog nauwelijks grootschalig was beproefd en dat er nog geen inzicht was in de gevolgen op het gebied van privacy en maatschappelijke acceptatie. Latere *pilots* bevestigden de bruikbaarheid van biometrie ter verbetering van identiteitscontrole aan de hand van reisdocumenten. Op basis *daarvan* achtte men biometrie tevens een geschikt middel ter bestrijding van *look-alike* fraude (maar dus zonder dit daadwerkelijk, op realistische wijze te hebben getest). Hetzelfde geldt voor later, gecontroleerd laboratorium- en literatuuronderzoek. Een en ander zou dus wel in theorie zijn 'aangetoond', maar niet in de praktijk. Dit gold eveneens voor de biometrieproef '2b or not 2b', aangezien het hier een volstrekt gecontroleerde situatie met vooraf geselecteerde vrijwilligers betrof. Bij deze laatste biometrieproef bleek bovendien dat er sprake was van een flinke foutmarge, zeker waar het de verificatie van biometrie (met name vingerafdrukken) betrof. Verder zijn in de parlementaire geschiedenis geen harde cijfers en statistieken over identiteitsfraude (inclusief *look-alike* fraude) bekendgemaakt.

Desalniettemin werd besloten om te kiezen voor invoering van de vingerscan in reisdocumenten (en gelaatsherkenning voor internationale grenspassage), met als primair doel de bestrijding van *look-alike* fraude.

Tenslotte kan nog worden opgemerkt dat de uitgevoerde biometrische 'kinderproef' op gespannen voet stond met relevant internationaal recht (in het bijzonder de rechten van het kind), zeker waar het kinderen betrof die te jong waren om met de proef te kunnen instemmen.

2.12 Overtrokken vlucht: het wetsvoorstel ter wijziging van de Paspoortwet in verband met de invoering van biometrie (2002)

2.12.1 Raad van State en CBP adviseren respectievelijk positief en negatief

Op 22 april 2002 diende (demissionair) minister voor Grote Steden- en Integratiebeleid Van Boxtel bij de Tweede Kamer een wetsvoorstel in ter wijziging van de Paspoortwet in verband met de toepassing van biometrische gegevens in de Nieuwe Generatie Reisdocumenten.[156] Toepassing van biometrie zou alleen worden toegestaan ter identificatie van de houder van het reisdocument. Ook zouden de biometrische gegevens in de (decentrale) reisdocumenten-administratie uitsluitend kunnen worden geraadpleegd op naam van de houder of het nummer van het aan de houder verstrekte document. Hiermee werd voorkomen dat willekeurig gezocht zou kunnen worden op de biometrische gegevens van personen. Over het oorspronkelijke wetsvoorstel had de Raad van State op 20 maart 2002 positief advies uitgebracht, gevolgd door een nader Rapport van minister Van Boxtel d.d. 16 april 2002. De lichte kritiek van de Raad betrof voornamelijk delegatiebepalingen en het ontbreken van een definitie van 'biometrische kenmerken' in het wetsvoorstel. Zo gaf de Raad de voorkeur aan regeling op wetsniveau (in plaats van bij tijdelijke algemene maatregel van bestuur, AMvB) van onderwerpen zoals het type biometrische kenmerken dat in de reisdocumenten zou worden opgenomen, in elk geval zodra de internationale ontwikkelingen terzake zouden zijn uitgekristalliseerd. Verder zou de verstrekking van biometrische gegevens uit de (decentrale) reisdocumentenadministratie aan daartoe bevoegde autoriteiten voor een deel op wetsniveau dienen te worden geregeld en voor het overige niet op een lager niveau dan bij AMvB (in plaats van bij ministeriële regeling). Blijkens het Nader Rapport zijn het wetsvoorstel en de memorie van toelichting aangepast overeenkomstig het advies van de Raad.[157]

Tekstbox 2.5

Door het College bescherming persoonsgegevens (CBP) was in oktober 2001 een negatief advies over het wetsvoorstel uitgebracht:

> "Het CBP is er niet van overtuigd, dat de tijd al rijp is om een wettelijke basis te leggen voor de toepassing van biometrie in reisdocumenten. Mocht daarover anders worden geoordeeld, dan is het gewenst om het kader voor de verwerking van biometrische gegevens op hoofdlijnen in de wet zelf neer te leggen en niet over te laten aan een nadere regeling bij algemene maatregel van bestuur. Daarbij moeten strakke grenzen worden gesteld met het oog op de bescherming van de persoonlijke levenssfeer. Wat het reisdocument zelf betreft beveelt het CBP aan om zorg te dragen voor een zodanige compartimentering en afscherming dat een onbevoegd gebruik van biometrische gegevens onmogelijk wordt gemaakt en dat in elk geval overneming in andere systemen is uitgesloten. *Het CBP acht het niet noodzakelijk om biometrische gegevens op te nemen in de administraties van de autoriteiten die bevoegd zijn tot de afgifte van reisdocumenten*. Mocht daarover anders worden geoordeeld, dan is het essentieel uit te gaan van een strikt doelgebonden gebruik van deze gegevens. Ook de beveiliging van deze gegevens verdient dan nadrukkelijke aandacht."[158]

In de latere memorie van toelichting bij het wetsvoorstel wordt slechts in een voetnoot naar (de parlementaire vindplaats van) dit advies verwezen.[159]

2.12.2 Het wetsvoorstel ingehaald door de tijd

De vaste Tweede-Kamercommissie voor Binnenlandse Zaken bracht op 10 juli 2002 haar verslag over het wetsvoorstel uit.[160] Kritische vragen werden met name gesteld door de GroenLinks-fractie, die de tijd voor dit wetsvoorstel (in de zin van de technische ontwikkeling van biometrie) nog niet rijp achtte; dit in navolging van het negatieve advies van het CBP.[161] Ook merkten de leden van deze fractie op dat "[o]pname van biometrische identificatie in alle reisdocumenten [een] inperking [kon] betekenen van de keuze van burgers om mee te werken aan opslag van biometrische gegevens en identificatiesystemen. Deze gevolgen zijn niet beschreven en deze leden weten voorshands niet in hoeverre de wet burgers kan dwingen danwel keuzevrijheid moet bieden. (...) Nergens wordt verder aangegeven hoever de verstrekking van biometrische gegevens in de interactie van burgers met de overheid en derden (dienstverleners, banken) mogelijk reikt."[162] Hierbij verwees de fractie nadrukkelijk naar het rapport *At face value* van de Registratiekamer (inmiddels CBP):

> "Wanneer dezelfde biometrische gegevens worden gebruikt voor allerlei verschillende handelingen, wordt het mogelijk om iemands leven voor een groot deel te traceren. Zeker bij toepassingen in de relatie overheid-burger is dit een punt van zorg omdat meestal de burger geen alternatief heeft."[163]

Vergelijkbare punten van kritiek werden geuit door de SP en de ChristenUnie.[164] Verder stelde GroenLinks een aantal vragen over de geplande decentrale opslag van biometrische gegevens, waaronder de vraag of die "decentrale gegevens centraal opvraagbaar [waren] en zo ja hoe en door wie?"[165] Ook vroeg GroenLinks zich af "[i]n hoeverre (...) het voornemen

van de regering [was] om opsporingsdiensten, politie, justitie, veiligheidsdiensten en de overheid toegang te verlenen tot de bestanden die zullen worden aangelegd, zowel centraal (administratief) als decentraal (de biometrische kenmerken)? Acht de regering het uitgesloten, mogelijk of wellicht zelfs wenselijk om biometrische gegevens (toekomstig) ter beschikking te stellen ten behoeve van de opsporing van (bepaalde vormen van) criminaliteit, staatsbedreigende activiteiten of illegalen?"[166] Door de PvdA werden overigens in het geheel geen vragen gesteld of opmerkingen gemaakt.

Na deze behandeling door de Tweede Kamer in juli 2002 raakte het wetsvoorstel snel verouderd, voornamelijk door politieke en technische ontwikkelingen rond biometrie in internationaal en Europees verband in 2003 en 2004 (waaronder de nieuwe ICAO-richtlijnen en de Europese paspoortverordening). Een en ander speelde destijds tegen de achtergrond van "verschillende terroristische aanslagen, die internationale ontwikkelingen op het terrein van biometrie in een stroomversnelling brachten en een sterke stimulans vormden voor een voortvarende aanpak om op internationaal niveau tot afspraken te komen over het gebruik van biometrie in reisdocumenten."[167] Een nota van de minister naar aanleiding van het verslag van de Tweede Kamer over dit wetsvoorstel is om deze redenen nooit uitgebracht.[168] In april 2005 werd aangekondigd dat het wetsvoorstel zou worden ingetrokken.[169] Dit gebeurde uiteindelijk in februari 2008,[170] nadat een nieuw wetsvoorstel terzake was ingediend.[171]

2.13 Biometrische doorstart: het wetsvoorstel ter wijziging van de Paspoortwet in verband met het herinrichten van de reisdocumentenadministratie (2008-2009)

2.13.1 Memorie van toelichting na negatief advies CBP en stilte bij Raad van State

In januari 2008 diende staatssecretaris van Binnenlandse Zaken Bijleveld (CDA) bij de Tweede Kamer een voorstel in tot wijziging van de Paspoortwet "in verband met het herinrichten van de reisdocumentenadministratie".[172] De door dit wetsvoorstel beoogde nieuwe (centrale) reisdocumentenadministratie zou 24 uur per dag, zeven dagen per week, online raadpleegbaar worden "met als voornaamste doel het creëren van een betrouwbaar aanvraag- en uitgifteproces van reisdocumenten met het oog op het voorkomen van identiteitsfraude."[173] Het tweede hoofdargument voor deze wetswijziging was dat van 'plaatsonafhankelijke dienstverlening'. Blijkens de memorie van toelichting zou het Nederlandse parlement hier in het kader van de lastenverlichting voor de burger al langere tijd op hebben aangedrongen.[174] Verder zou de wetswijziging voortvloeien uit de Europese paspoortverordening van december 2004.[175]

De memorie van toelichting stelde dat het primaire doel van de nieuwe reisdocumentenadministratie gelijk bleef aan dat van de bestaande administraties, namelijk het vastleggen van gegevens met betrekking tot alle Nederlandse reisdocumenten en het beschikbaar stellen van die gegevens aan de overheidsorganen en personen die belast waren met de uitvoering van de Paspoortwet. Daarnaast zouden echter tevens gegevens ter beschikking kunnen worden gesteld aan (bij algemene maatregel van rijksbestuur (AMvRB) aangewezen) organen en personen 'met het oog op:

a) het voorkomen en bestrijden van fraude met en misbruik van reisdocumenten;
b) de identificatie van slachtoffers van rampen en ongevallen;
c) de opsporing en vervolging van strafbare feiten en
d) het verrichten van onderzoek naar handelingen die een bedreiging vormen voor de veiligheid van de staat en andere gewichtige belangen van een of meerdere landen van het Koninkrijk dan wel de veiligheid van met het Koninkrijk bevriende mogendheden",[176] alsmede (ook aan derden) ter uitvoering van een wettelijke identificatieplicht.[177] Verder stelde de memorie van toelichting dat het onderhavige wetsvoorstel in wezen een verstrekkingenregime zou betreffen "dat in hoge mate vergelijkbaar is met dat in de huidige Paspoortwet en de daarop gebaseerde uitvoeringsregelingen, zij het dat er met onderhavig voorstel in de rijkswet zelf nadere regels worden opgenomen voor de verstrekking van gegevens uit de reisdocumentenadministratie."[178] Elders in de memorie van toelichting werd in dit kader onder andere verwezen naar het reeds bestaande artikel 73 van de Paspoortuitvoeringsregeling Nederland 2001 en naar artikel 126nc Wetboek van Strafvordering.[179] Tevens benadrukte de memorie dat "[i]n de nieuw te vormen reisdocumentenadministratie gegevens [worden] opgeslagen die nu in de decentrale reisdocumentenadministraties en het Basisregister Reisdocumenten zijn opgeslagen. Daaraan worden alleen de gegevens van de vingerafdrukken toegevoegd."[180]

Uit de biometrieproef '2b or not 2b' was volgens de memorie van toelichting gebleken dat de verificatie van vingerafdrukken bij 3% van alle personen niet slaagde (voornamelijk bij ouderen en mensen met zware beroepen). Om de kans op mislukking van verificatie van vingerafdrukken verder te verkleinen zou daarom zijn voorgesteld om twee extra (dus in totaal vier) vingerafdrukken in de reisdocumentenadministratie op te nemen.[181]

De vraag of de (nieuwe) centrale reisdocumentenadministratie veiliger zou zijn dan de (bestaande) decentrale administraties was blijkens de memorie van toelichting "niet eenduidig te beantwoorden".[182] Mogelijke risico's die inherent waren aan het centrale karakter van de administratie (zoals manipulatie ervan, of de administratie als 'single point of failure' bij uitval van het systeem) dienden volgens de regering te worden afgewogen tegen

de te nemen beveiligingsmaatregelen en tegen de huidige risico's van identiteitsfraude. "De weging van deze risico's heeft de [regering] tot het oordeel gebracht dat de mogelijkheid om fraude van en met reisdocumenten te kunnen voorkomen het zwaarste moet wegen en te kiezen voor een centrale reisdocumentenadministratie."[183]

Tekstbox 2.6

Het wetsvoorstel en de oorspronkelijke memorie van toelichting (alsmede een 'functioneel ontwerp') waren reeds in december 2006 door minister voor Bestuurlijke Vernieuwing Nicolaï ter advisering voorgelegd aan het CBP. In maart 2007 adviseerde het CBP negatief:

> "... [E]en centrale reisdocumentenadministratie met biometrische gegevens brengt voor de burgers ernstige en wellicht onnodige risico's voor de persoonlijke levenssfeer met zich, waartegen zij zich niet kunnen wapenen.
>
> 1. Het wetsvoorstel voldoet naar het oordeel van het CBP niet aan artikel 8 EVRM omdat een gedegen analyse van de voor- en nadelen van een centrale reisdocumentenadministratie ontbreekt. Alternatieven zoals een decentraal systeem met een centrale verwijsindex zijn niet besproken.
> 2. De hier beoogde centrale reisdocumentenadministratie is onomkeerbaar en zal de belangstelling krijgen van andere personen en organisaties vanwege de daarin opgeslagen persoonsgegevens. Het risico van 'function creep' [functieverschuiving] is aanwezig en het wetsvoorstel sluit dit niet uit.
> 3. Grootschalige toepassing van biometrie heeft vanwege technische onvolkomenheden ernstige gevolgen voor grote aantallen burgers.
> 4. De infrastructurele voorzieningen die internationaal nodig zijn om gegevens verantwoord uit te wisselen, zijn zeer ingrijpend en brengen beveiligingsrisico's met zich. Er wordt onvoldoende stilgestaan bij de vraag wat de gevolgen zijn wanneer er wordt 'ingebroken' in het systeem.
> 5. Er worden zowel nationaal als internationaal bedenkingen geuit tegen een centrale reisdocumentenadministratie met biometrische gegevens. Gewezen wordt op de risico's van misbruik, onjuist en onvoorzien gebruik. In de toelichting wordt onvoldoende een analyse gemaakt die erop gericht is deze bezwaren weg te nemen.

Gelet op het voorgaande betekent het voorliggende wetsvoorstel naar het oordeel van het CBP een *ernstige inbreuk* op de persoonlijke levenssfeer die niet wordt gerechtvaardigd door de door het wetsvoorstel te realiseren doeleinden."[184]

Naar aanleiding van de bezwaren van het CBP was de memorie van toelichting op enkele plaatsen aangevuld, voornamelijk door in de tekst een analyse van de voor- en nadelen van een centrale reisdocumentenadministratie op te nemen.[185] Uit deze analyse werd geconcludeerd dat "de invoering van een decentraal systeem met een centrale verwijsindex als een onwerkbare optie moet worden beschouwd."[186] Op enkele andere bezwaren van het CBP (*function creep*, misbruik, onjuist en onvoorzien gebruik) werd slechts in één pagina van de memorie van toelichting ingegaan.[187] De overige bezwaren van het CBP (over inherente technische en beveiligingsrisico's) liet de memorie van toelichting vrijwel geheel onbenoemd.[188] Wel werd erkend dat "de in een databank opgeslagen vingerafdrukken en foto's die verband houden met een gestolen identiteitsdocument (...) de werkelijke eigenaar

van die identiteit onophoudelijk grote problemen [kunnen] bezorgen. Biometrische gegevens zijn per definitie niet geheim en kunnen sporen achterlaten waardoor die gegevens verzameld kunnen worden zonder dat de eigenaar zich daarvan bewust is."[189]

De Raad van State had geen inhoudelijke opmerkingen naar aanleiding van het wetsvoorstel.[190]

2.13.2 Behandeling van het wetsvoorstel in de Tweede Kamer

Een eerste verslag van de Tweede-Kamercommissie voor Binnenlandse Zaken naar aanleiding van het wetsvoorstel verscheen eind maart 2008.[191] Door meerdere partijen werden de doelen, de privacy en de veiligheid van de centrale reisdocumentenadministratie aan de orde gesteld. Ook informeerden het CDA en de SP naar de samenhang tussen de modernisering en centralisering van de Gemeentelijke Basisadministratie (GBA) en de plaatsonafhankelijke uitgifte van reisdocumenten uit de centrale reisdocumenten-administratie. Verder vroegen de SP, SGP, VVD en CU hoe zou worden omgegaan met burgers die zouden weigeren om hun vingerafdrukken af te staan in verband met gemoeds- of gewetensbezwaren.[192] Op deze laatste vraag antwoordde de staatssecretaris in juli 2008 dat de Europese verordening geen ruimte liet voor gewetensbezwaarden en dat een regeling terzake haar bovendien onwenselijk leek: "Een dergelijke mogelijkheid bestaat immers ook niet ten aanzien van de opname van de foto in een reisdocument. Het voorzien in een dergelijke mogelijkheid doet afbreuk aan de doelstelling om onder meer *look-alike* fraude met reisdocumenten te voorkomen, bijvoorbeeld wanneer gewetensbezwaren worden voorgewend door degenen die fraude willen plegen met reisdocumenten."[193] Op de vragen over de samenhang met (en eventuele afhankelijkheid van) de nieuwe GBA antwoordde de staatssecretaris dat de modernisering van de GBA inderdaad een voorwaarde was voor de invoering van plaatsonafhankelijke dienstverlening met betrekking tot reisdocumenten. Voor het plaatsonafhankelijk aanvragen en uitreiken van reisdocumenten was het immers noodzakelijk om de actuele persoonsgegevens van de burger aan de balie te kunnen raadplegen en gebruiken. De gemoderniseerde GBA maakt het voor gemeenten mogelijk om on-line over de gegevens van burgers uit andere gemeenten te kunnen beschikken.[194]

Tekstbox 2.7

Reeds in april 2006 was uit onderzoek in opdracht van agentschap BPR gebleken dat plaatsonafhankelijke dienstverlening juist zou kunnen leiden tot een *toename* van identiteitsfraude:

> "Als belangrijkste risico voor de invoering van [plaatsonafhankelijke] dienstverlening wordt door de betrokken gemeenten fraude genoemd. Het gevaar bestaat dat kwaadwilligen gaan

shoppen, dat wil zeggen op zoek gaan naar gemeenten waar men het gemakkelijkst aan reisdocumenten kan komen."[195]

Negatieve adviezen op Europees niveau

Op Europees niveau waren over centrale opslag van biometrie negatieve adviezen uitgebracht door zowel de Europese Toezichthouder voor gegevensbescherming als door de Artikel 29-werkgroep van Europese privacytoezichthouders:

Tekstbox 2.8

Eind maart 2008 bracht de Europese Toezichthouder voor gegevensbescherming (EDPS) een negatief advies uit over centrale opslag van biometrische gegevens in het kader van de uitvoering van de Europese paspoortverordening:

> "Volgens een diepgaande studie die de [Artikel 29-werkgroep[196]] op verzoek van de commissie LIBE van het Europees Parlement heeft uitgevoerd over de uitvoering van Verordening (EG) nr. 2252/2004, hebben verscheidene lidstaten plannen voor het opzetten van een centrale gegevensbank voor de opslag van biometrische gegevens van het paspoort. *Hoewel de lidstaten alleen een procedure voor verificatie van biometrische gegevens middels een centrale gegevensbank kunnen invoeren, overeenkomstig de strenge beperking in de verordening, houdt deze optie bijkomende risico's in voor de bescherming van de persoonsgegevens*, zoals het ontstaan van verdere, niet in de verordening voorziene doelen, of zelfs visexpedities in de gegevensbank die moeilijk te bestrijden zullen zijn.
>
> De EDPS beveelt de [Europese] Commissie aan verdere harmonisatiemaatregelen voor te stellen zodat er *alleen gedecentraliseerde opslag wordt ingevoerd (in de draadloze chip van het paspoort)* betreffende biometrische gegevens die worden verzameld voor paspoorten van de lidstaten van de EU."[197]

Reeds in september 2005 had de Artikel 29-werkgroep in hetzelfde kader negatief geadviseerd over (Europese en nationale) centrale opslag van biometrische gegevens:

> "Het risico bestaat dat door het opzetten van een gecentraliseerde database met de persoonsgegevens, en in het bijzonder de biometrische gegevens, van alle (Europese) burgers inbreuk wordt gemaakt op het fundamentele evenredigheidsbeginsel. Elke centrale database zou ook een groter risico voor misbruik en oneigenlijke toe-eigening met zich meebrengen. Bovendien zou ook de kans op oneigenlijk gebruik en functieverschuiving toenemen. Tenslotte zou ook de mogelijkheid dat biometrische identificatiemiddelen worden gebruikt als 'toegangscode' voor diverse databases, waardoor gegevensbestanden aan elkaar zouden worden gekoppeld, erdoor toenemen."[198]

Nadere motivatie voor de centrale reisdocumentenadministratie

Naar aanleiding van vragen van de VVD en de PvdA over de Europese paspoortverordening antwoordde de staatssecretaris dat daarin niets was geregeld over de administraties die de lidstaten voeren voor reisdocumenten noch over de gegevens die in die administraties werden opgeslagen.[199] Gevraagd naar een nadere motivatie voor een centrale reisdocumentenadministratie in plaats van decentrale administraties met een centrale verwijsindex noemde zij als argumenten 1) fraudebestrijding, 2) plaatsonafhankelijke uitgifte, 3) efficiëntie in gebruik van de biometrische zoekfunctie en analyse van zoekresultaten, 4)

betere beschikbaarheid (vergeleken met mogelijk gebrekkige beschikbaarheid van (alle 700) decentrale administraties), 5) tijdwinst, 6) betere verwerkingscapaciteit en piekbelasting, 7) efficiënter periodiek onderhoud en 8) betere beveiliging, coördinatie en management.[200] Overigens zou het (in 2001 ingevoerde, 'negatieve') Basisregister Reisdocumenten ophouden te bestaan.[201]

Tekstbox 2.9

In haar nota van 16 juli 2008 aan de Tweede Kamer stelde de staatssecretaris tevens dat "pas met de bouw van de nieuwe administratie begonnen [wordt] als uit de discussie in het parlement duidelijk is geworden dat er voldoende steun bestaat voor de uitgangspunten van het wetsvoorstel. Daarmee kan worden voorkomen dat de technische opzet van de administratie als gevolg van de behandeling van het wetsvoorstel aangepast moet worden."[202] Interessant is in dit verband een eerder bericht uit de Volkskrant van 24 februari 2006:

> "Het ministerie van Binnenlandse Zaken werkt aan een databank met gelaatsscans en vingerafdrukken van alle Nederlanders met een paspoort. Daarmee worden de Eerste en Tweede Kamer gepasseerd, die de wetswijziging nog niet hebben goedgekeurd. Dit wordt bevestigd door deskundigen die bij de aanleg van de computerinfrastructuur zijn betrokken. Directeur Fons Knopjes van ID Management Centre, de organisatie die het ministerie van Binnenlandse Zaken bijstaat bij de bouw van de databank, spreekt van een 'dakpanconstructie'. Knopjes: 'De procedures en de werkzaamheden overlappen elkaar.' Een woordvoerder van het ministerie zegt dat er hard wordt gewerkt aan een wetsvoorstel, maar dat er nog geen datum is geprikt voor de behandeling daarvan in de Tweede Kamer."[203]

Vragen over (staats)veiligheid

Op een vraag van de PvdA naar het doel en nut van de nieuwe reisdocumentenadministratie met betrekking tot de staatsveiligheid antwoordde de staatssecretaris dat (betere mogelijkheden tot) het detecteren en voorkomen van identiteitsfraude zowel in het kader van criminaliteitsbestrijding als het voorkomen van terrorisme van groot maatschappelijk belang waren. "Het is de regering bekend dat het gebruik van vervalste reisdocumenten nog steeds onderdeel is van de *modus operandi* van terroristen," aldus de staatssecretaris.[204]

Op vragen van CDA en PvdA naar de beveiliging van de centrale reisdocumentenadministratie antwoordde de staatssecretaris onder meer als volgt:

> "... risico's met betrekking tot de integriteit van de gegevens in de administratie [zullen] zich evenzeer bij een decentrale opzet als bij een centrale opzet voordoen. Indien een 'inbreker' in staat is in één of enkele decentrale administraties in te breken en daar gegevens te manipuleren vormt dat niet een incident op zich. Er kan dan op geen enkele decentrale administratie meer worden vertrouwd. Het is immers ongewis waar en hoeveel inbraken hebben plaatsgevonden of nog zullen plaatsvinden en welke gegevens er dan zijn gemanipuleerd."[205]

Evenals de decentrale administraties zou de centrale reisdocumentenadministratie uitsluitend te benaderen zijn via besloten netwerken. Bovendien zouden alle organisaties met

toegang tot de nieuwe administratie zich digitaal moeten authenticeren met een certificaat. "De autorisatie is vastgelegd op organisatieniveau. Een functionaris van een organisatie kan alleen die functionaliteit van de administratie gebruiken waartoe de organisatie is geautoriseerd. De organisatie is zelf verantwoordelijk voor de autorisatie en beveiliging van de eigen systemen zodat alleen geautoriseerde gebruikers/functionarissen gebruik kunnen maken van de reisdocumentenadministratie."[206]

Vragen over de reisdocumentenadministratie als opsporingsregister

De CDA-fractie wilde weten waarom het in het wetsvoorstel niet mogelijk was gemaakt om van de gegevens in de reisdocumentenadministratie gebruik te maken bij de opsporing van *alle* misdrijven en overtredingen. In tegenstelling hiermee vroeg de SP juist of de centrale database in de praktijk geen opsporingsregister zou worden, en of er geen sprake zou zijn van *datamining*. De staatssecretaris antwoordde hierop onder andere als volgt:

> "In het voorgestelde artikel 4b, vierde lid, is de grens voor verstrekking van biometrische kenmerken aan de officier van justitie ten behoeve van strafrechtelijk onderzoek gelegd bij de misdrijven waarvoor voorlopige hechtenis is toegelaten. Voor die grens is gekozen omdat daarmee wordt aangesloten bij het in het Wetboek van Strafvordering vastgelegde uitgangspunt dat dwangmiddelen die een inbreuk maken op de lichamelijke integriteit, alleen kunnen worden bevolen in geval van verdenking van een strafbaar feit waarvoor voorlopige hechtenis is toegelaten. Verder wordt met de grens van voorlopige hechtenis aangesloten bij de huidige werkwijze van identiteitsvaststelling door tal van politiekorpsen. Volgens deze werkwijze worden van verdachten die in verzekering zijn gesteld, altijd foto's en vingerafdrukken genomen. Het bevel tot inverzekeringstelling kan slechts worden verleend in geval van een strafbaar feit waarvoor voorlopige hechtenis is toegelaten. Voor de duidelijkheid wijs ik erop dat artikel 4b van het wetsvoorstel op dit punt een bijzondere regeling is ten opzichte van artikel 126nc van het Wetboek van Strafvordering."[207]
>
> "De regering deelt niet de zorg van de leden van de SP-fractie dat de reisdocumentenadministratie in de praktijk een opsporingsregister zal worden, omdat de mogelijkheden om de reisdocumentenadministratie te raadplegen in het kader van strafbare feiten in de wet heel duidelijk is ingeperkt. Slechts voor de identiteitsvaststelling van verdachten en veroordeelden, in het kader van de toepassing van het strafrecht dan wel in het belang van het onderzoek in geval van een misdrijf waardoor voorlopige hechtenis is toegelaten (...) kunnen uit de nieuwe reisdocumentenadministratie biometrische gegevens worden verstrekt.
>
> Het is ook van belang om het misverstand uit de weg te ruimen dat het openbaar ministerie in het belang van onderzoek naar strafbare feiten de reisdocumentenadministratie zou kunnen gebruiken om uitsluitend op basis van vingerafdrukken die in het kader van sporenonderzoek gevonden zijn, naar een identiteit te zoeken. Dergelijk gebruik van de reisdocumentenadministratie is niet beoogd en zal ook niet mogelijk worden gemaakt bij algemene maatregel van rijksbestuur. De officier van justitie moet het geslacht van de betrokkene weten en een gezichtsopname en vingerafdrukken hebben. Alleen met deze drie gegevens van een betrokkene zal de officier van justitie in geval van een misdrijf waarvoor voorlopige hechtenis is toegelaten (...) in de reisdocumentenadministratie kunnen nagaan of betrokkene een reisdocument heeft of heeft gehad en onder welke identiteit. Voor de duidelijkheid wijs ik er bovendien op dat van het verlenen van 'toegang' tot de reisdocumentenadministratie geen sprake is, maar alleen van de verstrekking van gegevens. Er is gelet op het voorafgaande geen sprake van *datamining*."[208]

Vragen over het foutenpercentage van vingerafdrukken

De SP en SGP vroegen hoe groot het foutenpercentage was van de vingerafdrukken die zouden worden verzameld en of gevreesd moest worden dat dit percentage groter werd naarmate de bestanden groter werden. De staatssecretaris antwoordde hierop als volgt:

> "De bestanden van de reisdocumentenadministratie worden hoe dan ook groter. Per jaar worden er namelijk meer dan 3 miljoen reisdocumenten aangevraagd. De gegevens van die aanvragen worden opgeslagen in de reisdocumentenadministratie, ook als er sprake is van decentrale bestanden. [Eerder] is reeds uitvoerig ingegaan op de maatregelen die ter beveiliging van de gegevens in de reisdocumentenadministratie worden getroffen en welke voordelen een centrale administratie daarbij biedt ten opzichte van een decentrale variant."[209]

Vragen over het maatschappelijk draagvlak

Verder vroeg de SGP-fractie zich af of er recent nog onderzoek was gedaan naar de bezwaren die naar hun indruk leefden tegen biometrische gegevensopslag, naar de vraag of de weerstand was toe- of afgenomen en op welke vragen die weerstand zich richtte. De staatssecretaris:

> "Er is geen specifiek onderzoek hiernaar gedaan. Het is duidelijk dat er bezwaren bestaan tegen het gebruik van biometrie en chiptechnologie in onder meer de reisdocumenten. De koninkrijksregering is evenwel van mening dat alles overwegende de beveiliging van de reisdocumenten met deze technieken een goede zaak is. Daarom is, ook voordat de Europese Unie hieromtrent voorstellen had gedaan, reeds besloten om toe te werken naar de invoering van biometrische kenmerken in de reisdocumenten. Door de ontwikkelingen in de Europese Unie, in casu de Europese verordening die in 2004 door de Raad is aanvaard, is de chip in de reisdocumenten met daarin de gezichtsopname en de vingerafdrukken een uitgemaakte zaak. De reisdocumentenadministratie bevat nu reeds biometrische gegevens, te weten de gezichtsopname en de handtekening. In de praktijk is niet gebleken dat daartegen bezwaren bestaan."[210]

Tekstbox 2.10

In de zomer van 2007 hadden het Rathenau Instituut, de Consumentenbond en ECP.nl gezamenlijk kwalitatief en kwantitatief onderzoek gedaan naar het Nederlandse maatschappelijke bewustzijn en de maatschappelijke acceptatie van RFID-technologie. Hieruit was onder meer gebleken dat het voornemen van elektronische opslag van vingerafdrukken op de RFID-chip in het biometrische paspoort door 80% van de Nederlanders als (zeer) goed werd beoordeeld. Verder bleek 66% van de Nederlanders voor centrale (door opsporingsinstanties te raadplegen) opslag van vingerafdrukken, 20% was daar tegen, en 56% was voor centrale opslag van gelaatsscans (26% was tegen).

Ook centrale opslag van gelaatsscans om mensen op videobeelden te kunnen identificeren werd door 62% als (zeer) goed beoordeeld en door 14% als (zeer) slecht.[211]

Vraag over een nader standpunt van het CBP

Door de PvdA was tenslotte nog gevraagd of het CBP, na de aanvulling in de memorie van toelichting inzake het alternatief van decentrale opslag met een centrale verwijsindex, zich

inmiddels op dit punt alsnog had kunnen vinden in het wetsvoorstel. De staatssecretaris antwoordde:

> "Aan het [CBP] is advies gevraagd in de totstandkomingsfase van het wetsvoorstel. Aan de opmerking om een analyse te maken van de voor- en nadelen van een centrale reisdocumentenadministratie is gevolg gegeven door de [memorie van] toelichting op dit punt aan te vullen. Uit deze analyse blijkt dat een stelsel van decentrale reisdocumenten-administraties niet wenselijk is, gelet op de eisen van raadpleegbaarheid en beschikbaarheid. Aan het CBP is vervolgens niet opnieuw om advies gevraagd. Ik beschik dan ook niet over informatie of het CBP zich inmiddels wel kan verenigen met het wetsvoorstel op dit punt."[212]

Eerste openbaar debat

In november 2008 volgde het eerste debat over het wetsvoorstel in de Tweede Kamer. Kritiek tijdens dit debat was vooral afkomstig van de SP, die het wetsvoorstel onvoldragen, onuitgewerkt en onduidelijk achtte.[213] De PvdA liet weten positief tegenover het wetsvoorstel te staan en had nog slechts enkele praktische vragen plus een opmerking over privacy die een citaat waard is:

> "Het [CBP] adviseerde in eerste instantie negatief, maar de aanpassingen waar dat advies toe heeft geleid in het huidige wetsontwerp leidden bij mij tot de conclusie dat er ten opzichte van de huidige situatie niets verandert. Er is alleen mogelijkheid tot inzage bijgekomen die kan worden gevorderd door een officier van justitie ten behoeve van identiteitsvaststelling in geval van een misdrijf waarvoor voorlopige hechtenis is toegelaten. Met andere woorden: *er verandert niets ten opzichte van de huidige rechtsbescherming van personen. Daarmee is voor ons de privacy in voldoende mate gewaarborgd.*"[214]

D66 leek beter geïnformeerd:

> "Ik heb toch mijn twijfels bij het voorliggende wetsvoorstel. De centrale reisdocumenten-administratie zal veel privacygevoelige informatie bevatten. Gezichtsopnames en vingerafdrukken zijn hier voorbeelden van. Wie weet wat er in de toekomst nog meer bij komt. *Dat leidt eigenlijk voor mij tot een heel principiële vraag: kan de staatssecretaris garanderen dat in de toekomst niet ook andere gegevens, zoals DNA zullen worden toegevoegd?* Kan ik dat de staatssecretaris wel vragen? Weten wij wel of deze stap niet vanzelf tot meer gaat leiden? Dat is iets waar ik in ieder geval veel meer moeite mee zou hebben." (...) Ik ben kritisch over de toegang van de officier van justitie tot deze gegevens. Wij moeten oppassen dat de centrale opslag niet een soort opsporingsregister wordt. De officier van justitie kan een foto, vingerafdrukken en het geslacht van de verdachte doorgeven aan de beheerder van de centrale administratie. Vervolgens worden deze gegevens door de beheerder vergeleken met de centrale administratie. Wie is deze beheerder? Hoeveel zijn het er? Welke bevoegdheden zijn er?[215]

GroenLinks maakte een vergelijkbaar punt:

> "Wanneer deze centrale reisdocumentenadministratie eenmaal is gecreëerd, zullen er, zo leert de praktijk, nieuwe doeleinden en gebruiken ontstaan. Dit is het bekende 'function creep'(...). Dat is een gevaar. Dat is een risico waarop de staatssecretaris in de nota naar aanleiding van het verslag niet ingaat, terwijl het wel een reëel gevaar is voor de toekomst. (...) Als het centrale databestand er is – misschien nog niet volgend jaar, misschien wel het jaar daarop – kan zij niet voorkomen dat andere organisaties en andere personen met legitieme doelen, daar niet van, belangstelling krijgen voor deze gegevens. Wellicht zullen zij er met behulp van het democratisch proces toch in slagen om het bedoelde gebruik van de databank verder op te rekken, wat niet de bedoeling was van de staatssecretaris."[216]

Een ander relevant onderwerp werd door de VVD herhaald:

> “De staatssecretaris stelt wel heel erg veel AMvB’s voor. De vraag is of het niet verstandig is, haar de ruimte te geven om hiermee door te gaan. Dat is mogelijk via het goedkeuren van het wetsvoorstel, maar het is ook mogelijk dat wij nog eens bekijken wat wij echt in de wet vastleggen wanneer er echte keuzen zijn gemaakt. In de techniek van wetgeving zitten erg veel variabele gegevens en het is niet goed dat al die gegevens door haar alleen worden ingevuld. Op een aantal cruciale punten zal de Kamer hieraan te pas moeten komen, zeker als de reikwijdte wordt verbreed.”[217]

Opmerkelijk was verder het voorstel van de PVV:

> “Wij kunnen onze steun verlenen aan deze Paspoortwet, maar ik heb wel een belangrijk amendement ingediend (...). Mijn amendement wil namelijk regelen dat de officier van justitie voor de opsporing en vervolging van misdrijven waarop een voorlopige hechtenis staat, de beschikking krijgt over *alle vingerafdrukken* uit de centrale reisdocumentenadministratie. *Ook in het geval van sporenonderzoek zou de officier van justitie daarover de beschikking moeten krijgen.* Verstrekking van vingerafdrukken via een verzoek van de officier van justitie is dan niet meer nodig, omdat hij met dit amendement gewoon de beschikking krijgt over alle vingerafdrukken in de centrale reisdocumentenadministratie.”[218]

De VVD reageerde hierop als volgt:

> “Ik kan mij voorstellen dat je met die ene vingerafdruk die je hebt gevonden naar de beheerder [van de centrale reisdocumentenadministratie] toegaat en hem vraagt om die afdruk tegen zijn bestand aan te houden en te melden van wie die vingerafdruk is.”[219]

Hieronder volgt een selectie van opvallende fragmenten uit de (gedeeltelijke) beantwoording door staatssecretaris Bijleveld tijdens het plenaire debat:

> “Bij de behandeling van het wetsvoorstel [over het ‘negatieve’ Basisregister Reisdocumenten in 2000] is al met de Kamer gesproken over de invoering van een positieve reisdocumentenadministratie, een administratie van alle reisdocumenten met vermelding van de status van die documenten. De toenmalige regering zag de voordelen van een dergelijke administratie (...). Maar men wilde eerst resultaten van de invoering van de nieuwe generatie reisdocumenten boeken.”[220]

> “De uitgevende instanties van de reisdocumenten – de gemeenten, ambassades, et cetera – zijn (...) groot voorstander van de nieuwe administratie. Zij zitten er als het ware op te wachten.”[221]

> “Ik wil ten slotte in dit algemene deel nog een enkele opmerking over de privacy maken. Het is heel belangrijk om te onderstrepen dat het primaire doel van en de mogelijkheden om gegevens te verstrekken uit de reisdocumentenadministratie niet wezenlijk verschillen van de bestaande reisdocumentenadministraties. Het primaire doel blijft immers om gegevens vast te leggen met betrekking tot alle Nederlandse reisdocumenten en deze gegevens beschikbaar te stellen aan de autoriteiten die belast zijn met de uitvoering van de Paspoortwet, voor zover deze gegevens noodzakelijk zijn voor de vervulling van hun taken. (...) In die zin kan er dan ook geen sprake zijn van een inbreuk op de privacy ten gevolge van de nieuwe reisdocumentenadministratie. (...) De vervanging van de papieren administraties door een centrale digitale administratie heeft geen negatieve gevolgen voor het niveau van privacybescherming. Uitvoeringsinstanties krijgen bijvoorbeeld niet meer rechten dan voorheen om gegevens op te vragen door de invoering van de nieuwe reisdocumentenadministratie.”[222]

"Waarom is in veel bepalingen gekozen voor nadere regels bij AMvB of ministeriële regeling, vroegen de heren Van Beek [VVD] en Pechtold [D66]. Eigenlijk is het tegenovergestelde het geval. In het wetsvoorstel wordt juist op veel punten bepaald de nader te stellen regels niet langer te stellen op het niveau van een ministeriële regeling, maar op het niveau van een AMvRB. Dat is een verbetering ten opzichte van wat er nu is."[223]

"De heer Van Raak [SP] en anderen hebben vragen gesteld over de zogenaamde *function creep*. In het wetsvoorstel staat nauwkeurig omschreven voor welke doelen gegevens kunnen worden verstrekt en aan welke voorwaarden organen moeten voldoen om voor gegevensverstrekking in aanmerking te komen. (...) De uitwerking van de regels bij algemene maatregel van rijksbestuur kan niet plaatsvinden buiten de in het wetsvoorstel gestelde doelen en kaders. De woordvoerders moeten daarnaar nog maar eens goed kijken. Voor een eventuele verruiming van de mogelijkheden tot gegevensverstrekking dient eerst de wet te worden gewijzigd. Als het daarvan komt, zal de Kamer daarbij altijd opnieuw betrokken zijn. De Kamer zal dus altijd een oordeel moeten geven over zo'n verruiming van mogelijkheden. (...) Mijns inziens bevat het wetsvoorstel echt voldoende waarborgen om gegevensverstrekking buiten de wettelijk omschreven doelen te voorkomen. Bovendien zijn ook de waarborgen uit de [Wbp] van toepassing, waaronder het toezicht door het [CBP]. In het licht van dit kader is het risico op een *function creep* mijns inziens niet groot. Bij algemene maatregel van rijksbestuur kan alleen binnen de grenzen van de wet een nadere uitwerking worden gegeven aan de vraag aan wie gegevens specifiek kunnen worden verstrekt. Zo is het geregeld."[224]

Vraag over een eventueel (biometrie)relevant verdrag

Een aantal resterende vragen beantwoordde de staatssecretaris enkele dagen later per brief.[225] Tevens beantwoordde zij hierbij een vraag die GroenLinks had gesteld bij de regeling van de werkzaamheden op 18 november 2008:

"[GroenLinks] vroeg aan de minister van Justitie en aan mij (...) in te gaan op de overeenkomst die op Europees niveau zou bestaan over paspoorten en in het bijzonder over de database voor vingerafdrukken en daarbij de consequenties aan te geven voor het onderhavige wetsvoorstel. Een overeenkomst *in EU-verband* is [mij echter] niet bekend. (...)"[226]

Vragen over het verstrekkingenregime

Tijdens het Kamerdebat over het wetsvoorstel waren diverse vragen gesteld over de delegatiebepalingen met betrekking tot de gegevensverstrekking uit de reisdocumenten-administratie. Ter verduidelijking kwam de staatssecretaris hier nogmaals op terug:

"a. *De doelen van gegevensverstrekking*
Uitgangspunt is dat gegevensverstrekking alleen mogelijk is voor de doelen, genoemd in artikel 4b, eerste en tweede lid. Valt de taak van een instantie niet binnen een van de wettelijke doelen, dan is gegevensverstrekking niet toegestaan. De doelen waarvoor gegevens worden verstrekt, kunnen *niet* worden uitgebreid in de lagere regelgeving op grond van de Paspoortwet. Verstrekking buiten de regeling in de Paspoortwet is alleen mogelijk voor zover een andere wet de Paspoortwet opzij zet.

b. Welke instanties komen precies in aanmerking voor gegevensverstrekking, komen ook niet-overheidsinstanties daarvoor in aanmerking?
Welke instanties concreet gegevens verstrekt kunnen krijgen, wordt wat betreft de verstrekking van gegevens voor de uitvoering van de Paspoortwet reeds bepaald in de wet zelf, op grond van artikel 4b, eerste lid. Voor zover het gaat om verstrekking voor de doeleinden, genoemd in artikel 4b, tweede lid, kan dit nader worden bepaald bij algemene maatregel van rijksbestuur. Omdat de verdeling van taken over de verschillende instanties van tijd tot tijd kan wijzigen, is het noodzakelijk de aanwijzing van de instanties op die wijze te regelen. Het

wetsvoorstel geeft daarbij de kaders, de algemene maatregel van rijksbestuur kan zich *niet* buiten die kaders bewegen.

Het moet dan gaan om:
- overheidsorganen, die een taak uitoefenen waarvoor gegevens uit de reisdocumentenadministratie noodzakelijk zijn (artikel 4b, derde lid, onder a), of
- instellingen en personen die met het oog op een wettelijke identificatieplicht een gerechtvaardigd belang hebben bij verstrekking van gegevens uit de reisdocumentenadministratie (artikel 4b, derde lid, onder b).

Bij beide categorieën geldt uiteraard nog steeds de voorwaarde dat verstrekking alleen mogelijk is indien de taakuitoefening van de betreffende instellingen en personen valt binnen de hiervoor genoemde doelen. Zowel het doel van de gegevensverstrekking als de kaders voor de aanwijzing van de concrete instanties die recht hebben op gegevensverstrekking vinden derhalve een grondslag in het wetsvoorstel. Er is dus in feite sprake van een dubbel slot op de gegevensverstrekking. Met betrekking tot de gegevensverstrekking aan AIVD en MIVD geldt artikel 17 van de Wet op de inlichtingen en veiligheidsdiensten. Dit artikel voorziet erin dat de wettelijke beperkingen op grond van de Paspoortwet niet van toepassing zijn op die gegevensverstrekking aan deze diensten.

(...) Hierbij wil ik er nogmaals op wijzen dat in beginsel alle overheidsorganen die voor de uitoefening van hun taken gegevens nodig hebben uit de reisdocumentenadministratie daarvoor al op basis van de bestaande wet- en regelgeving in aanmerking komen.

Daarnaast voorziet het wetsvoorstel in een zeer beperkte gegevensverstrekking aan instellingen en personen die een belang hebben bij de verkrijging van gegevens in het kader van de uitvoering van een wettelijke identificatieplicht. Alleen bij die categorie instanties kan het ook gaan om niet-overheidsorganen, voor zover die organen wettelijk verplicht zijn in bepaalde gevallen de identiteit van een betrokkene vast te stellen. Dit kunnen bijvoorbeeld banken en kredietverstrekkers zijn. Door de verstrekking van gegevens te binden aan de voorwaarde dat zij gevraagd moeten worden in het kader van de uitvoering van een wettelijke identificatieplicht, is ook in dit geval sprake van een dubbel slot. Ik merk hierbij op dat de in dit wetsvoorstel voorgestelde regeling op dit onderdeel zelfs beperktere mogelijkheden biedt dan de huidige wet. Op grond van het bestaande artikel 4a, zevende lid, kan verstrekking van gegevens als hier bedoeld plaatsvinden aan instellingen en personen die daarbij een gerechtvaardigd belang hebben. De eis dat het moet gaan om de uitvoering van een wettelijke identificatieplicht wordt op dit moment derhalve niet gesteld.” [227]

Een en ander werd nog verder verduidelijkt bij brief van begin december 2008; een bijlage daarbij bevatte een overzicht met betrekking tot alle delegatiebepalingen in het wetsvoorstel.[228] Hieruit bleek voor vrijwel alle nadere regelgeving een hoger delegatieniveau dan voorheen (namelijk van ministeriële regelingen naar algemene maatregelen van rijksbestuur).

Geen uitzondering voor principieel bezwaarden

Tijdens het Kamerdebat had de VVD erop gewezen dat noodpaspoorten (zonder vingerafdrukken) geen ‘escape’ zouden mogen worden voor mensen die geen vingerafdrukken in het reisdocument willen. De staatssecretaris “deel[de] deze zorg. Het zal duidelijk zijn dat het niet is toegestaan om de opname van de vingerafdrukken voor een reisdocument te weigeren. De opname van vingerafdrukken in een paspoort en in een Nederlandse identiteitskaart is verplicht op grond van de EU-verordening.”[229] Zij hield rekening met “de situatie dat personen een tijdelijke beperking (bijvoorbeeld verwondingen)

aanwenden om zich te onttrekken aan het opnemen van vingerafdrukken. Bij een tijdelijke beperking waardoor geen van de vingerafdrukken kunnen worden opgenomen zal ik daarom betrokkene een reisdocument met een geldigheidsduur van 1 jaar (in plaats van 5 jaar) verstrekken."[230]

Uitspraak van het EHRM in de zaak Marper v. UK

Tijdens de parlementaire behandeling van het wetsvoorstel deed het Europese Hof voor de Rechten van de Mens (EHRM) een belangwekkende uitspraak:

Tekstbox 2.11

Het Europese Hof voor de Rechten van de Mens deed op 4 december 2008 uitspraak in de zaak *Marper v. UK*. Deze zaak had betrekking op twee Britten wier DNA en vingerafdrukken in het kader van een strafrechtelijke procedure waren afgenomen en opgeslagen in een databank van de Britse overheid. Beiden waren vervolgens ontslagen van rechtsvervolging. Hun vingerafdrukken, DNA-materialen en DNA-profielen bleven echter voor onbepaalde tijd in de databank opgeslagen. Het EHRM oordeelde dat dit in strijd was met het recht op eerbiediging van de persoonlijke levenssfeer *ex* art. 8 EVRM.[231]

Op 18 december 2008 vroeg de vaste commissie voor Binnenlandse Zaken aan de staatssecretaris om te reageren op de recente uitspraak van het EHRM in de zaak *Marper v. UK* en de eventuele consequenties van deze uitspraak aan te geven voor het in behandeling zijnde wetsvoorstel. De staatssecretaris antwoordde hierop als volgt:

> "Het EHRM concludeert in de uitspraak over de zaak Marper-UK dat het ongelimiteerd opslaan en bewaren van (onder meer) vingerafdrukken van personen die verdacht waren, maar niet zijn veroordeeld, in een database met vingerafdrukken van verdachten, in strijd is met artikel 8 van het EVRM.
>
> Juist de *strafrechtelijke context* van het opslaan en bewaren van de vingerafdrukken tezamen met de omstandigheid dat er geen grenzen zijn gesteld inzake de ernst van het strafbare feit en de duur van het opslaan, maakt dat het Hof het als een zware inbreuk ziet op de privacy, bedoeld in artikel 8. Het Hof meent dat er geen goede argumenten zijn aangevoerd die een dergelijke inbreuk rechtvaardigen.
>
> Op grond van het voorliggende wetsvoorstel worden – anders dan in de casus waarover de uitspraak gaat – de vingerafdrukken echter niet opgeslagen in een strafrechtelijke context, maar in het kader van de uitgifte van reisdocumenten. De registratie van vingerafdrukken in de reisdocumentenadministratie geldt in beginsel voor iedere aanvrager van een reisdocument en heeft derhalve als zodanig geen enkel stigmatiserend effect. Daarmee verschilt de opslag van vingerafdrukken in de reisdocumentenadministratie wezenlijk van de registratie van vingerafdrukken van verdachte personen in een politieel of justitieel register. Dit laat onverlet dat vingerafdrukken, die in de reisdocumentenadministratie zijn opgeslagen, in voorkomende gevallen beschikbaar kunnen worden gesteld voor het identificeren van verdachten. In het wetsvoorstel zijn in dat verband overigens duidelijke grenzen gesteld: de verstrekking van vingerafdrukken kan slechts in een beperkt aantal gevallen plaatsvinden, en alleen aan de officier van justitie.

> Uit de uitspraak van het Hof in de zaak Marper-UK blijkt verder dat er bij de opzet van de registratie niet of in onvoldoende mate een afweging was gemaakt tussen enerzijds het private en anderzijds het publieke belang. Die afweging is bij de reisdocumentenadministratie wel gemaakt. De toelichting bij het voorstel tot wijziging van de Paspoortwet gaat uitvoerig in op de vraag waarom het belang van een accurate en effectieve reisdocumentenadministratie het opslaan van vingerafdrukken rechtvaardigt. Gelet op het voorafgaande ben ik van mening dat de uitspraak in de zaak Marper-UK geen consequenties heeft voor de voorgenomen wijziging van de Paspoortwet."[232]

Tweede openbaar debat

Tijdens het tweede plenaire debat over het wetsvoorstel (januari 2009) werd op initiatief van het CDA, PvdA en VVD voornamelijk ingegaan op de kosten en enkele andere praktische punten rond het toekomstige paspoort, waaronder het in Europees verband in te voeren beginsel van '1p:1p' (één persoon per paspoort, ook bij (jonge) kinderen).[233] Door de SP werden nogmaals vragen gesteld over de delegatiebepalingen, reikwijdte, privacy, beveiliging en *datamining*.[234] D66 vroeg de staatssecretaris onder andere om nader in te gaan op de betekenis van *Marper v. UK* en was "nog niet helemaal overtuigd van delen van dit wetsvoorstel. [Men zag] zeker het nut van een centrale reisdocumentenadministratie. De vraag [bleef] echter of de voordelen opwegen tegen de nadelen en de risico's."[235] GroenLinks had voornamelijk vragen over doelbinding, *function creep* en foutmarges. Ook vond GroenLinks dat *Marper v. UK* gevolgen voor dit wetsvoorstel moest hebben. "Het gaat bij dit wetsvoorstel immers niet alleen om verdachten, zoals bij de zaak Marper-UK, maar ook om de vingerafdrukken van alle Nederlanders. Dat lijkt [GroenLinks] een veel vergaander en verruimde toepassing."[236] De staatssecretaris antwoordde dat de centrale reisdocumentenadministratie niet voor *datamining* zou mogen worden gebruikt en dat dit ook niet zou *kunnen* (dus ook niet door de AIVD):

> "Ten slotte wijs ik erop dat er geen sprake is van het verlenen van rechtstreekse toegang tot de reisdocumentenadministratie. Er kan daarin dan ook niet vrijelijk worden gezocht, noch kunnen er vrijelijk gegevens worden verzameld. Dit is het punt van *datamining*, waarover de [SP] het net had. Er is slechts sprake van welomschreven, specifieke verstrekking van gegevens."[237]

Met betrekking tot alle delegatiebepalingen en het eventueel 'voorhangen' van AMv(R)B's bij de Kamer maakte de staatssecretaris de volgende opmerkingen:

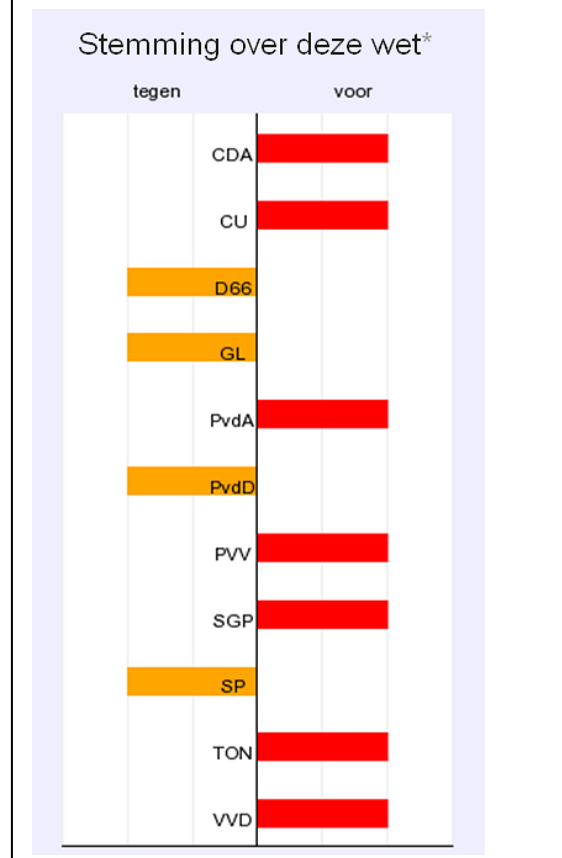
> "Ik ben in het algemeen niet meteen een voorstander van voorhangprocedures. Als de Kamer constateert dat de gedelegeerde wetgeving niet goed werkt, kan zij mij altijd ter verantwoording roepen. (...) Ik waag te betwijfelen of voorhangen van die AMvB nog iets toevoegt. De Kamer heeft een heel duidelijk inzicht in wat er gebeurt."[238]

Verder zag de staatssecretaris geen risico van *function creep*.[239] Haar eerdere argumenten naar aanleiding van *Marper v. UK* werden door de staatssecretaris min of meer herhaald,[240] en over foutmarges kon zij nog niets zeggen:

> "Wij moeten nog beginnen met de invoering, wij moeten de apparatuur en programmatuur nog testen, ik kan u nu echt nog niet zeggen wanneer ik u iets kan doen toekomen over de foutmarges. Daar moet je toch minstens een jaar mee hebben gewerkt. Maar ik zal er eens over nadenken."[241]

Op deze punten werd tijdens het debat vervolgens niet meer doorgevraagd.

Figuur 2.1 Stemming over deze wet



Aanname van het wetsvoorstel

Op 20 januari 2009 werd het wetsvoorstel door de Tweede Kamer aangenomen. PvdA, VVD, ChristenUnie, SGP, CDA, PVV en het lid Verdonk stemden voor.[242] Het voorgestelde amendement van de PVV om de officier van justitie de beschikking over alle vingerafdrukken te geven werd slechts gesteund door de PVV en het lid Verdonk. Hetzelfde gold voor een motie van de PVV om het dragen van een hoofddoek op de pasfoto voor reisdocumenten te verbieden.[243]

2.13.3 Behandeling van het wetsvoorstel in de Eerste Kamer

Op dezelfde dag dat de Tweede Kamer het wetsvoorstel aannam, werd het bij de Eerste Kamer ingediend.[244] Eind maart 2009 werd het voorlopig verslag over dit wetsvoorstel door de vaste Eerste-Kamercommissie voor Binnenlandse Zaken vastgesteld.[245] Dit verslag bevatte een aantal vragen van het CDA, PvdA, VVD, SP, SGP, CU en D66, voornamelijk over de beveiliging, de keuze voor centrale in plaats van decentrale opslag en de toegang tot het systeem. (Door GroenLinks werden ditmaal geen vragen gesteld of opmerkingen gemaakt.) Vragen over de beveiliging van centrale opslag tegen *hackers* werden gesteld door de PvdA, SP en D66.[246] In dit verband vroeg D66 bovendien welke rechtsbescherming aan getroffen burgers zou worden geboden.[247] De VVD merkte op dat "Nederland (…) – voor zover bekend – het enige land [is] dat gekozen heeft voor een centraal register" en vroeg (evenals de SP) waarom niet gekozen was voor decentrale opslag met een centrale verwijsindex.[248] Vragen over *function creep* werden gesteld door de SGP, CU, D66 en SP.[249] Vragen over de feilbaarheid en foutmarges van biometrie werden vervolgens gesteld door de SGP, CU en

D66.[250] Door D66 werd verder gevraagd naar de rechtvaardigende *pressing social need* alsmede de proportionaliteit en subsidiariteit van de inbreuk op de privacy van de burger bij gebruik van biometrische gegevens uit de centrale reisdocumentenadministratie door de officier van justitie. D66 miste bij de regering een concrete belangenafweging terzake en beriep zich hierbij ook op de bevindingen van het CBP.[251] De SP stelde in dit verband eveneens de proportionaliteit en functionaliteit van het wetsvoorstel aan de orde.[252] Volgens de regering zou de uitspraak in de zaak *Marper v. UK* geen consequenties hebben voor dit wetsvoorstel, omdat de opslag van biometrische gegevens (vingerafdrukken) van alle burgers in een centrale administratie niet in een strafrechtelijke context zou geschieden. D66 vroeg zich "desalniettemin af waarom de officier van justitie dan toegang wordt verleend tot deze database. Creëert dit dan niet een strafrechtelijke context?"[253]

> "Krijgt de centrale reisdocumentenadministratie, nu de Officier van Justitie de biometrische gegevens kan ontvangen bij bepaalde misdrijven, in feite ook niet de functie van een opsporingsregister, zo vragen de leden van de fracties van de SGP en CU. Vormt deze consequentie niet een ernstige inbreuk op de persoonlijke levenssfeer, omdat ook de gegevens van niet verdachte burgers worden opgenomen in de registers?"[254]

Op de centrale reisdocumentenadministratie zou de Wbp van toepassing zijn. Het CDA vroeg in dit verband hoe burgers zouden worden voorgelicht over hun eventuele mogelijkheden van bezwaar en beroep in verband met de opslag van hun gegevens.[255] Een vraag over de kosten van de nieuwe reisdocumenten werd gesteld door de PvdA.[256] Door de SP werd tenslotte nog gevraagd naar de uitvoeringsmaatregelen ter nadere invulling van de wet.[257]

Beveiliging en rechtsbescherming

Eind april 2009 werden de vragen uit het voorlopig verslag door staatssecretaris Bijleveld beantwoord.[258] Met betrekking tot de beveiliging en rechtsbescherming rond de centrale reisdocumentenadministratie antwoordde zij onder andere:

> "Het is helaas nooit 100 procent uit te sluiten dat onbevoegden toegang krijgen tot de gegevens. Niet is op voorhand aan te geven welke gevolgen dat zal hebben voor de individuele burger die in de reisdocumentenadministratie is geregistreerd. Indien mocht blijken dat als gevolg van de onrechtmatige toegang de burger schade heeft geleden, dan zal van geval tot geval bekeken moeten worden wie aansprakelijk kan worden gesteld voor deze schade."[259]

Nadere motivatie voor een centrale reisdocumentenadministratie

De keuze voor centrale in plaats van decentrale opslag was volgens de staatssecretaris (met verwijzing naar de memorie van toelichting en de Nota naar aanleiding van het verslag) "primair ingegeven vanuit de noodzaak om het aanvraag- en uitgifteproces van de Nederlandse reisdocumenten betrouwbaarder te maken. Secundair heeft meegewogen het streven om, in het kader van de vermindering van administratieve lasten voor burgers, het aanvragen van een reisdocument plaatsonafhankelijk te maken."[260]

Verder zou de keuze voor een decentrale opzet volgens de staatssecretaris een aantal nadelen met zich meebrengen, namelijk:

1. bij een decentrale opzet zouden ongeveer 700 administraties in plaats van 1 administratie online raadpleegbaar moeten worden gemaakt;
2. de bij een decentrale opzet benodigde centrale verwijsindex zou veel gegevens moeten gaan bevatten die ook in de decentrale administraties opgeslagen waren;
3. elke biometrische zoekopdracht ter voorkoming van identiteitsfraude zou naar alle decentrale administraties dienen te worden gezonden;
4. ook bij een decentrale opzet zou een centrale voorziening nodig zijn om de resultaten van de biometrische zoekfunctie te kunnen analyseren (deze expertise zou immers niet beschikbaar kunnen zijn bij alle 700 decentrale instanties);
5. bij een decentrale opzet zou er een risico zijn dat niet alle decentrale administraties continu online beschikbaar zouden zijn;
6. gegevensverwerking via een centrale verwijsindex en decentrale administraties zou meer tijd vergen dan via één centrale administratie;
7. door concentratie van de verwerkingscapaciteit zou bij een centrale opzet de piekbelasting efficiënter kunnen worden georganiseerd;
8. vergroting van de verwerkingscapaciteit zou bij een centrale opzet een investering op één plek vergen in plaats van op 700 plekken;
9. hetzelfde zou gelden voor onderhoud en aanpassingen; een centrale opzet zou hierbij ook een betere waarborg bieden voor de functionele continuïteit van het hele systeem;
10. een centrale opzet zou beter (en uniformer) te beveiligen zijn dan een decentrale opzet.[261]

Vergelijking met andere Europese landen

Op een vraag van de VVD in hoeverre de ervaringen van andere landen met decentrale administraties waren betrokken in de afweging om over te gaan tot centrale opslag, antwoordde de staatssecretaris als volgt:

> "*De regering beschikt niet over een overzicht van de wijze waarop andere landen centraal dan wel decentraal registers hebben ingericht voor de administratie van hun reisdocumenten. In EU-verband heeft overleg dan wel uitwisseling van informatie hierover niet plaatsgevonden.* De oorzaak hiervoor is dat de EU-verordening geen betrekking heeft op de opslag van de gegevens in het kader van het aanvragen en uitgeven van de reisdocumenten. Verder speelt een rol dat de wet- en regelgeving in de lidstaten van de Unie (en overigens ook daarbuiten) sterk van elkaar verschilt wat een zinvolle vergelijking in de weg staat. Welke keuzes de landen hebben gemaakt en wat de achtergronden daarbij zijn geweest is dus niet geïnventariseerd en heeft derhalve ook geen rol gespeeld in afweging [*sic*] die de regering heeft gemaakt."[262]

Figuur 2.2

Country	Centralised	Decentralised
AT	Yes	
BE	Yes	
CZ	Yes	
DE		Yes
ES	Yes	
ET	Yes	
FI	Yes	
HU	Yes	
IS	Yes	
LU	Yes	
NL		Yes
PT	Yes	
SI	Yes	
SK	Yes	
SW	Yes	
UK		Yes

Bij dit antwoord van de staatssecretaris hadden destijds wellicht enkele vraagtekens kunnen worden geplaatst. Begin maart 2009 was door het Portugese ministerie van Binnenlandse Zaken immers een vergelijkend onderzoek gepubliceerd naar identiteitsregistratie in Europa. (Dit onderzoek was na een Europese conferentie in november 2007 onder Portugees EU-voorzitterschap geïnitieerd. Het onderzoek was uitgevoerd door het Nederlandse ID Management Centre in Den Haag, waarbij onder andere gebruik was gemaakt van informatie van het IF4TD.) Aan 30 Europese landen waren vragenlijsten over diverse kwesties toegezonden; deze vragenlijsten werden vervolgens door 22 landen (waaronder 19 EU-lidstaten) ingevuld geretourneerd. Eén van de vragen had betrekking op de centrale en/of decentrale opslag van biometrische gegevens uit identiteitsdocumenten. Hieruit bleek dat reeds in veel Europese landen sprake zou zijn van centrale opslag van biometrie in een nationale database. (Vooralsnog zou het hierbij echter vooral gaan om gezichtsscans. Slechts in Tsjechië, Spanje, Portugal, Slowakije en Zwitserland zou reeds sprake (geweest kunnen) zijn van centrale opslag van vingerafdrukken.) Slechts in drie landen was sprake van decentrale opslag van biometrie: Duitsland, Nederland en het Verenigd Koninkrijk. Zie ook de figuur hiernaast (afkomstig uit het betreffende onderzoeksrapport; de landen zijn aangegeven door middel van ISO-codes).[263] Op initiatief van de huidige EU-voorzitter België zouden momenteel voorbereidingen worden getroffen voor aanvullend, actueel onderzoek. Dit Belgische initiatief zou naar verwachting in oktober 2010 met de Europese Commissie worden besproken.[264]

Intrinsieke fouten en rechtsbescherming

Over intrinsieke fouten in biometrie en rechtsbescherming stelde de staatssecretaris het volgende:

> “Elke techniek, ook biometrie, heeft onvolkomenheden. Bekend is dat een verificatie van de burger aan de hand van vingerafdrukken niet altijd mogelijk is. Dat is niets nieuws want met gezichtsopnamen die nu al in het reisdocument en de administratie zijn opgenomen is het niet anders. De combinatie van gezichtsopname en vingerafdrukken maakt het echter wel mogelijk meer zekerheid te krijgen bij de identiteitsverificatie. Maar ook dan zal er nooit voor de volle 100 procent op kunnen worden vertrouwd. (...) Wat de gevolgen zullen zijn van intrinsieke fouten in de biometrie is niet eenduidig aan te geven. Dit zal afhankelijk zijn van de situatie

> waarin dit gegeven wordt geraadpleegd. Evenals in het geval van onrechtmatige toegang tot gegevens als gevolg van *hacke*n, geldt ook hier dat, indien mocht blijken dat de burger schade heeft geleden, van geval tot geval zal moeten worden bekeken wie daarvoor aansprakelijk kan worden gesteld."[265]

Proportionaliteit en subsidiariteit

Op de vragen over de proportionaliteit, subsidiariteit en functionaliteit van het wetsvoorstel in het licht van art. 8 EVRM antwoordde de staatssecretaris als volgt:

> "Om de gevolgen van het [wetsvoorstel] voor de privacy in kaart te brengen, is van belang de situatie zoals deze voorafgaand aan het wetsvoorstel is, in ogenschouw te nemen. De doelen en mogelijkheden om gegevens te verstrekken uit de nieuwe reisdocumentenadministratie ingevolge het wetsvoorstel verschillen niet wezenlijk van die van de bestaande reisdocumentenadministraties [ingevolge de bestaande Paspoortwet en reeds daarop gebaseerde uitvoeringsregelingen]. (...) In die zin kan er dan ook geen sprake zijn van een inbreuk op de privacy ten gevolge van het onderhavige voorstel van rijkswet. Wat wel verandert is het volgende. Ten eerste worden er straks naast de bestaande gegevens ook de vingerafdrukken van de houder in reisdocumenten opgenomen en geregistreerd in de reisdocumentenadministratie. Het opnemen van vingerafdrukken in reisdocumenten vloeit voort uit Verordening (EG) nr. 2252/2004. Het opnemen van vingerafdrukken in reisdocumenten en het opslaan daarvan is inderdaad een inbreuk op de bescherming van de persoonlijke levenssfeer. Die inbreuk is naar mijn mening gerechtvaardigd, met name omdat deze leidt tot een meer betrouwbaar en effectief aanvraag- en uitgifteproces van reisdocumenten. Fraude met reisdocumenten, zoals look-alike-fraude, kan daarmee beter worden bestreden. In de memorie van toelichting ben ik uitgebreid ingegaan op die afweging. Van belang is dat de registratie van vingerafdrukken met voldoende waarborgen is omkleed. Dat is in het onderhavige wetsvoorstel het geval, onder meer doordat zeer nauwkeurig is beschreven voor welke doeleinden de gegevens mogen worden gebruikt."[266]

Strafrechtelijke context

Naar aanleiding van de vragen over de "strafrechtelijke context" van de centrale reisdocumentenadministratie antwoordde de staatssecretaris (nogmaals) als volgt:

> "De centrale reisdocumentenadministratie krijgt in verband met de verstrekking in bepaalde gevallen van vingerafdrukken aan de officier van justitie niet het karakter van een opsporingsregister of een register met een strafrechtelijke context. Anders dan in het geval van registers met een strafrechtelijke context is het criterium om persoonsgegevens te registreren niet de vraag of de betrokkene een strafrechtelijk verleden heeft, maar de vraag of de betrokkene in het bezit is van een reisdocument. Dat is dan ook een belangrijk verschil met de registratie, waarop de zaak Marper-UK betrekking had. De registratie van vingerafdrukken in de reisdocumentenadministratie geldt in beginsel voor iedere aanvrager van een reisdocument en heeft derhalve als zodanig geen enkel stigmatiserend effect."[267]

Publieksvoorlichting

Op de vraag over (publieksvoorlichting omtrent) mogelijkheden van bezwaar en beroep rond de gegevensopslag in de centrale reisdocumentenadministratie, antwoordde de staatssecretaris dat gemeenten bij de aanvraag van een nieuw reisdocument een folder aan de burger meegaven waarin "onder meer [staat] dat het document zorgvuldig gebruikt moet worden en wordt aangegeven wat de burger moet doen bij diefstal of vermissing van zijn document. (...) Vanzelfsprekend zal *op het moment dat de centrale reisdocumentenadministratie wordt ingevoerd* de tekst in de folder worden uitgebreid met

een korte uiteenzetting over het opnemen en het gebruik van de gegevens in deze administratie alsmede de rechten van de burger ten aanzien van zijn opgeslagen gegevens.”[268]

Nadere regelgeving en ‘function creep’

Op de vraag naar de kosten van nieuwe reisdocumenten werd geantwoord dat de ontwikkeling en het beheer van de centrale reisdocumentenadministratie hierin zouden worden doorberekend. Volgens een voorlopige schatting zouden de kosten per document hierdoor met € 3,50 à € 4,00 stijgen.[269] Op de vraag welke uitvoeringsmaatregelen (met name AMvRB’s) waren gepland waarvan de Eerste Kamer kennis zou moeten nemen, antwoordde de staatssecretaris: “[d]e zaken, waarvan kennisneming door uw Kamer naar mijn mening wenselijk is, zoals de doelen waarvoor gegevensverstrekking mogelijk is uit de nieuwe reisdocumentenadministratie, zijn op het niveau van rijkswet geregeld.”[270] Tenslotte antwoordde zij tevens dat “het risico van *function creep*, voor zover daarbij de wettelijke doelbinding in gevaar komt, naar mijn mening (...) niet aanwezig [is].”[271]

Openbaar debat

Nadat de vaste commissie voor Binnenlandse Zaken vervolgens had laten weten dat zij de openbare behandeling van het wetsvoorstel voldoende voorbereid achtte,[272] volgde het debat erover in de Eerste Kamer.

Tekstbox 2.12

Een dag voor het debat uitten een aantal wetenschappers in een brief[273] aan de Eerste Kamer hun ernstige bezwaren tegen de aanname van de nieuwe Paspoortwet, waaronder:

- het feit dat de nieuwe Paspoortwet veel verder ging dan de Europese verordening;
- de risico’s van opslag van biometrie buiten het document;
- het feit dat technische alternatieven (zoals ‘hashing’ in plaats van ‘templates’) onvoldoende waren onderzocht;
- de aantasting van de privacy zonder redelijk vermoeden van schuld;
- het gevaar van *function creep*;
- inherente technische risico’s (waaronder foutmarges) en schaalfouten;
- het gebrek aan noodzakelijkheid.

Tijdens het openbare debat in de Eerste Kamer op 9 juni 2009 werden veel eerder gestelde vragen door partijen herhaald of aangevuld. Zo vroeg de VVD nogmaals hoe groot de kans was

dat vingerafdrukken niet correct aan de juiste personen gekoppeld zouden worden en de rechtsbescherming ter zake, ook bij gevallen van *hacking*. “Is [de staatssecretaris] bereid een centraal aanspreekpunt aan te wijzen voor gedupeerde burgers?”[274] De SP zette haar toon voor het debat als volgt:

> “Het heeft er enige schijn van dat bewindslieden die zich ooit met ons paspoort bemoeiden statistisch een grote kans maken hier in de Eerste Kamer te eindigen. (...) Dus alvast welkom voor later, mevrouw de staatssecretaris. Het is deze maand 21 jaar geleden dat de Tweede Kamer besloot tot een parlementaire enquête naar de gang van zaken rondom de opvolger van wat toen ‘het zwarte vod’ heette: een naam die werd gebruikt om aan te duiden dat het toenmalige paspoort op een achternamiddag door een knappe knutselaar kon worden nagemaakt.”[275]

De SP herhaalde vervolgens haar eerder gemaakte punt over de nadere, nog onduidelijke uitwerking van het wetsvoorstel door middel van 23 aanvullende regelingen (veelal AMvRB’s) en stelde vervolgens ook (voor de eerste maal expliciet) het punt van dit wetsvoorstel als ‘nationale kop’ op Europese regelgeving aan de orde, bijvoorbeeld door het gebruik van de opgeslagen gegevens bij opsporing en vervolging en bij onderzoek in het kader van binnenlandse en buitenlandse staatsveiligheid. “Kan het zo zijn dat deze gegevens aan bevriende mogendheden worden overgedragen, bijvoorbeeld aan de Verenigde Staten? Onder welke voorwaarden zou dat gebeuren? (...) Als het kabinet besluit om deze mogelijkheden in de toekomst te verruimen, gaat dat dan per wet of per AMvB? Dat is nogal van belang, omdat in het laatste geval deze Kamer daar vermoedelijk niets meer over te zeggen zou hebben.”[276] Verder vroeg de SP zich onder andere af waarom de staatssecretaris er niet voor had gekozen om het gewijzigde wetsvoorstel (c.q. de memorie van toelichting die na de kritiek van het CBP aangevuld was met een belangenafweging) opnieuw naar het CBP te sturen. Evenals de VVD vroeg de SP tenslotte ook opnieuw aandacht voor de beveiliging:

> “Elk paspoort valt na te maken. En het zijn vooral boeven die daartoe lust blijken te hebben. Dat zal met dit paspoort niet anders zijn. Ondertussen werkt Brussel al aan een driedimensionale foto. Zo blijven we nog wel even bezig; en de boeven dus ook.”[277]

Ook de SGP herhaalde haar eerdere zorgen over de doelen en reikwijdte van het wetsvoorstel en de beveiliging van een en ander.[278] D66 ging met name (nogmaals) in op de privacy-aspecten, ook in het licht van art. 8 EVRM en de zaak *Marper v. UK*. Verder vroeg D66 zich af of het wetsvoorstel niet in strijd was met de Europese paspoortverordening:

> “Als biometrische kenmerken gebruikt worden door de officier van justitie om een verdachte in een strafonderzoek te identificeren, levert dit dan geen schending op van de Europese verordening? (...) Reiken de doeleinden die door de regering zijn geformuleerd in artikel 4b van het wetsvoorstel, niet veel verder dan de verordening toestaat?”[279]

De nieuwe Paspoortwet als nationale kop op Europese wetgeving

GroenLinks wees in haar betoog allereerst op vermeende Nederlandse ‘chantage’ (eind 2004) van de Europees-parlementaire besluitvorming over de paspoortverordening.[280] Het feit dat het huidige wetsvoorstel veel verder ging dan deze verordening deed volgens GroenLinks tevens “de vraag rijzen of Nederland misschien niet helemaal zijn zin heeft gekregen in de Europese onderhandelingen, zijn voorstel heeft moeten afzwakken en daarom nu maar bij de implementatie nationale koppen introduceert. Is deze indruk juist en, zo ja, in hoeverre strijdt deze implementatiewetgeving met de afspraak om nationale koppen te vermijden?”[281] Andere vragen van GroenLinks hadden vooral betrekking op privacy, beveiliging en centrale versus decentrale opslag.[282] Vervolgens had de PvdA niet zozeer kritische vragen aan de staatssecretaris, als wel een aantal opmerkingen ter verdediging van het wetsvoorstel tegenover de SP, D66 en GroenLinks. Hieruit bleek overigens wel dat de PvdA eveneens bezwaar had “tegen koppen op internationale wetgeving zonder dat die nadrukkelijk geïdentificeerd en gerechtvaardigd worden in de toelichting. (...) Dat is hier voor drie onderwerpen het geval. (...) Ik neem aan dat de staatssecretaris vandaag zal uitleggen waarom die drie koppen in dit wetsvoorstel nodig zijn.”[283] Niettemin was de PvdA verder van mening dat “het Nederlandse volk hier heel blij mee zal zijn” en het “in het algemeen als een zegen [zou] ervaren.”[284] Vervolgens sprak het CDA eveneens enkele verdedigende woorden, waaronder de opmerking dat “ook het [CBP] in zijn advies buitengewoon positief [was] over de wijze waarop de aandacht voor beveiliging vorm heeft gekregen, ook al had zij op andere punten kritiek.”[285] Het CDA kon dan ook “niet meer doen dan de staatssecretaris succes wensen met de uitvoering.”[286]

Verdediging door de staatssecretaris vanuit Europees perspectief

Vervolgens hield de staatssecretaris eerst haar algemene inleiding. Ze maakte daarin enkele opvallende, nieuwe opmerkingen:

> “In 2001 zijn overigens ook *afspraken gemaakt* over de invoering van een positieve reisdocumentenadministratie waarin alle reisdocumenten zijn opgenomen met vermelding van alle statussen van die documenten van de aanvraag tot de vernietiging. (...) De voordelen van die positieve lijst werden toen al onderkend, maar er werd voor gekozen om eerst te bezien wat de resultaten waren van de nieuwe generatie reisdocumenten. (...) Wij hadden dus altijd al dit doel voor ogen, een centraal raadpleegbare reisdocumentenadministratie. (...) Wij waren (...) altijd al van plan om zo’n reisdocumentenadministratie op te zetten.”[287]

> “Met deze wijziging van de Paspoortwet wordt inderdaad iets anders geregeld dan in de Europese verordening is opgenomen, namelijk de opslag van deze gegevens in de reisdocumentenadministratie en de verstrekkingen die daaruit mogen plaatsvinden. Dit is echter geen schending van de verordening (...). De verordening is heel duidelijk op dit punt. Ik wijs op *overweging 5 van de gewijzigde verordening die op 6 juni 2009 in het Publicatieblad van de Europese Unie is gepubliceerd.* In de betreffende overweging staat namelijk het volgende: ‘Deze regeling laat ander gebruik of andere opslag van deze gegevens, in casu de biometrische gegevens, overeenkomstig de nationale wetgeving van de nationale lidstaat onverlet. De verordening voorziet niet in een rechtsgrondslag voor het opzetten of bijhouden

van gegevens[banken voor de opslag van deze gegevens] in de lidstaten. Dat is *louter* een nationale aangelegenheid.' Het is derhalve aan de lidstaat om eigen regelgeving te maken voor de opslag en het gebruik van de gegevens in de lidstaat. Dat is precies wat wij hebben gedaan in deze wijziging van de Paspoortwet. Dat is wat ons voor ogen stond."[288]

"Nederland is overigens niet het enige land in de EU met het voornemen om de vingerafdrukken op te slaan in een centrale administratie. Ik heb bij enkele lidstaten laten nagaan hoe zij omgaan met de opslag van vingerafdrukken voor reisdocumenten. Ik heb niet van iedereen een reactie ontvangen, maar van vier lidstaten heb ik de reactie ontvangen dat zij ook van plan zijn om die vingerafdrukken centraal op te slaan. Dat zijn *Finland, Griekenland, Frankrijk en Hongarije. Daarnaast werkt België er ook aan.* Wij zijn dus niet uniek met de manier waarop wij werken."[289]

"Het CBP heeft kritiek op het wetsvoorstel, maar het heeft op de beveiliging geen kritiek. Het college heeft zijn waardering uitgesproken voor de beveiligingsmaatregelen."[290]

"[Mij is] gevraagd hoe groot de kans is dat een vingerafdruk bij een verkeerde persoon in het reisdocument terechtkomt in de administratie. Die kans acht ik niet groot. Alle procedures, en ook de technische voorzieningen zoals de biometrische zoekfunctie in het centrale bestand, zijn zo ingericht dat dit moet worden voorkomen. Als een persoon desondanks wordt geconfronteerd met het feit dat een ander met zijn identiteit en vingerafdrukken rondloopt, zal moeten worden nagegaan wat er is gebeurd. Vanzelfsprekend zal de betrokken persoon in zo'n geval moeten worden geholpen bij het bewijzen van zijn identiteit. Als dat is gebeurd, moeten de registraties worden aangepast als er inderdaad verkeerd is geregistreerd. Dergelijke gevallen kunnen ook worden aangemeld bij het in december opgerichte Centraal Meldpunt Identiteitsfraude. Dit meldpunt zal de klacht van de burger in behandeling nemen en ervoor zorgen dat die bij de juiste instanties terechtkomt."[291]

Standpunt van het CBP

Verder liet de staatssecretaris (nogmaals) weten dat naar aanleiding van het negatieve advies van het CBP een belangenafweging in de memorie van toelichting was opgenomen. (Het wetsvoorstel zelf was intact gelaten.)[292] De staatssecretaris was in dit verband tevens gevraagd waarom zij het wetsvoorstel niet opnieuw aan het CBP had voorgelegd. "Dat is omdat wij vonden dat wij zijn ingegaan op het [*sic*] kritiek van het CBP. Wij hebben een nadere onderbouwing gegeven. (...) Wij hebben de belangenafweging duidelijk gemaakt. Ik heb die nog eens uitgebreid toegelicht. Ik vind het een goede afweging. De Kamer moet het zelf wegen, maar wij hebben wel degelijk serieus aandacht besteed aan datgene wat het CBP heeft ingebracht. Ik vind het ook niet nodig om dan nog een keer langs een adviesorgaan te gaan. Dat doen wij ook niet bij de Raad van State. Wij schrijven een nader rapport dat de Kamer moet beoordelen. Die procedure hebben wij met elkaar afgesproken, want anders kunnen wij voortdurend bij adviesorganen langs blijven gaan. Dat lijkt mij niet de bedoeling (...)."[293]

Veiligheid, rechtsbescherming en 'nationale koppen'

De staatssecretaris zegde toe dat er periodiek *hacker*-proeven zouden worden gedaan om de beveiliging van de centrale reisdocumentenadministratie te testen.[294] Over de rechtsbescherming voor de burger zei zij verder echter dat de overheid niet meteen de aansprakelijkheid voor schade zou erkennen. "Je moet wel kijken wie verantwoordelijk is."[295]

De staatssecretaris was zich “bewust van het feit dat wij daarvoor wel een regeling moeten maken.”[296]

Na een korte discussie tussen de VVD, D66 en GroenLinks over de belangenafweging terzake werd door de SP nogmaals kritiek geuit over het wetsvoorstel als nationale kop op Europese regelgeving.[297] Vervolgens liet de SGP weten het wetsvoorstel inmiddels te steunen. Daarentegen liet D66 weten dat “twijfel blijft bestaan of de mogelijke aantasting van de privacy voldoende evenredig en evenwichtig wordt afgewogen ten opzichte van het belang van de opslag en het gebruik van die biometrische gegevens en de doelstellingen waarvoor deze worden ingezet (...).”[298] GroenLinks bleef eveneens kritisch:

> “In het gesprek met de minister van Justitie over (...) nationale koppen heeft hij onderkend dat je niet in een- en dezelfde wet implementatiewetgeving en nationale beleidskeuzes moet regelen. Dat heeft natuurlijk voor een deel te maken met de transparantie. (...) Er is echter nog een ander argument. Als het in één wetsvoorstel zit, komen we in gewetensnood op het moment dat we het niet eens zijn met de beleidskeuzes. We voelen ons namelijk verplicht om akkoord te gaan met wetgeving waaraan de Nederlandse regering zich al heeft verbonden in Brussel, terwijl we daarmee tegelijkertijd ook akkoord gaan met keuzes waarmee we het niet eens kunnen zijn. Dat is nog een extra argument waarom het echt niet aanvaardbaar is om implementatiewetten en nationale koppen in één wetsvoorstel te verenigen.”[299]

De staatssecretaris beantwoordde vervolgens een resterende vraag van de VVD:

> “[De VVD] vroeg nog naar de kans dat het verkeerd gaat met de vingerafdruk. Ik heb die kans als klein aangemerkt. Ik kan dat moeilijk uitdrukken in percentages. Wij hebben er uitgebreid over gesproken. Ik denk dat die kans zeer klein tot vrijwel nihil is, gezien de wijze waarop wij het doen. Ik kan daar geen percentage voor noemen.”[300]

Hierna kwam(en) GroenLinks (en de SP) weer terug op het punt van ‘nationale koppen’:

> “[GroenLinks:] De principiële vraag is nu, of de staatssecretaris het eens is met haar collega Hirsch Ballin en met de regering als zij stellen dat je [een en ander] niet in dezelfde implementatiewet kunt regelen.
> [Staatssecretaris:] Laat ik het omdraaien. Mijn collega Hirsch Ballin is het er volledig mee eens dat wij wat nu voorligt in dit wetsvoorstel zo regelen. Daarover heb ik uitgebreid met hem gesproken.
> [GroenLinks:] Dat betekent dat de regering het niet met de Kamer eens is. Dat betekent dat de regering het standpunt huldigt dat je nationale koppen in een implementatiewet kunt opnemen.
> [Staatssecretaris:] Ik spreek alleen over dit geval en doe geen uitspraken over welke andere wet ook. Wij zijn van mening dat het in dit geval kan.
> [GroenLinks:] De staatssecretaris erkent dus dat er sprake is van nationale koppen?
> [Staatssecretaris:] Daarover heb ik in de eerste en de tweede termijn geen misverstand laten bestaan. Ja, dit is een nationale kop.
> [GroenLinks:] Ik concludeer dat de regering vindt dat je nationale koppen in een implementatiewet kunt opnemen. Dat kun je op z’n minst in sommige gevallen volgens de regering doen.
> [Staatssecretaris:] In dit geval. Ik bestrijd dat je dat in sommige gevallen kunt doen. Ik heb gesproken over dít geval. De conclusie van [GroenLinks] deel ik dus niet. Het gaat mij sec om dít geval.” [301]

Geen overleg over nationale opslag in EU-verband

Tenslotte deelde de staatssecretaris nog mee dat er "geen overleg *in EU-verband* [is] over opslag in nationale databanken. Dat hoeft ook niet, want in de verordening staat dat dit een zaak is van de lidstaten zelf, niet van de Europese Unie. Daarom is daarover geen overleg georganiseerd."[302]

Aanname van het wetsvoorstel zonder stemming

Hierna achtte de staatssecretaris alle vragen beantwoord en werd de beraadslaging gesloten. Vervolgens kwam het als volgt tot aanname van het wetsvoorstel:

> "[Voorzitter:] Wenst een van de leden stemming over het wetsvoorstel? Ik zie dat dit het geval is. Wij zullen volgende week over dit wetsvoorstel stemmen.
>
> De vergadering wordt enkele ogenblikken geschorst.
>
> [Voorzitter:] Ik vraag aandacht voor een misverstand zowel aan de kant van de regering als aan de kant van de Kamer. Het betreft de stemming over [dit wetsvoorstel]. Ik heb begrepen dat de Kamer het goedvindt dat er geen stemming plaatsvindt, maar dat er wel moet worden gesproken over aantekening. Ik herhaal daarom mijn vraag: wenst een van de leden stemming over dit wetsvoorstel? Ik zie dat dit niet het geval is. Verlangt een van de leden aantekening? Ik zie dat dit het geval is. De aanwezige leden van de fracties van D66, de SP en GroenLinks wordt conform artikel 121 van het Reglement van Orde aantekening verleend dat zij geacht willen worden zich niet met het wetsvoorstel te hebben kunnen verenigen."[303]

Tijdens het debat in de Eerste Kamer had de OSF zich laten vertegenwoordigen door D66. De PvdD liet zich vertegenwoordigen door de SP. Zowel de OSF, de PvdD als het lid Yildirim waren tegen het wetsvoorstel, maar door de plotseling vervroegde aanname ervan waren ze niet in de gelegenheid geweest om (evenals D66, SP en GroenLinks) aantekening te verlangen. In de vergadering de week daarna hebben deze partijen hun ongenoegen hierover laten blijken en alsnog in de Handelingen laten opnemen dat zij niet met de nieuwe Paspoortwet instemden:

> "[OSF]: Voorzitter. Wij hadden er vast op gerekend dat de stemming over de Paspoortwet die vorige week is behandeld, vandaag zou plaatsvinden. Daar waren afspraken over gemaakt en dat is ook de gebruikelijke gang van zaken. *Vanwege een of andere omstandigheid* is het zo niet gelopen en heeft de stemming over deze wet vorige week al plaatsgevonden. Voor mij, maar ook voor een aantal anderen, geldt dat wij daar niet op gerekend hadden. Als wij daarbij geweest waren, zouden wij aantekening hebben gevraagd. Die mogelijkheid hebben wij nu echter niet gehad. Ik wil dit graag op deze manier melden, zodat dit in de annalen van deze Kamer geboekstaafd is.
>
> [Voorzitter]: Mag ik u op één punt corrigeren? Er is vorige week niet gestemd over dit wetsvoorstel. Vandaar dat u aantekening had kunnen vragen.
>
> Het woord is aan [de PvdD].
>
> [PvdD]: Voorzitter. Ik sluit mij aan bij de woorden van de [OSF] dat het erg ongebruikelijk is dat er plotseling niet gestemd wordt over een wetsvoorstel en er dus ook geen aantekening gevraagd kan worden. Als mijn fractie aanwezig geweest was, had zij aantekening gevraagd.

> Dat geldt ook voor de fractie van de heer Yildirim. Ook wij willen dit graag opgenomen zien in de Handelingen.
>
> Deze mededelingen worden voor kennisneming aangenomen."[304]

Misleidende folder en 'verificatieverbod'

Het parlementaire debat over de nieuwe Paspoortwet leek hiermee vooralsnog te zijn afgerond. Wel volgde er op 17 september 2009 nog een brief van de staatssecretaris:

> "Van deze gelegenheid wil ik gaarne gebruik maken om nog enkele punten onder uw aandacht te brengen. Op 7 september 2009 is de huis-aan-huis verspreiding gestart van een *folder met daarin informatie over de opname van de vingerafdrukken in de Nederlandse reisdocumenten*. Op die zelfde datum is de website www.paspoortinformatie.nl voorzien van nieuwe informatie omtrent de vingerafdrukken. (...)
>
> Het, vanwege de invoering van de vingerafdrukken, aanpaste aanvraag- en uitgifteproces van de Nederlandse reisdocumenten wordt door [BZK] nauwgezet gevolgd om inzicht te krijgen in de eventuele knelpunten die zich in praktijk voordoen. Dat is van belang omdat het proces rond de opname van de vingerafdrukken, ook internationaal, nog in ontwikkeling is. *Een voorbeeld hiervan is de vraag of er vingerafdrukken, ongeacht de kwaliteit ervan, moeten worden opgenomen voor opslag in de reisdocumenten. De Europese Commissie is die mening toegedaan. Nederland staat hier kritisch tegenover.* Ik zal de Kamer over nieuwe ontwikkelingen op dit punt informeren. Bij het aanvragen van een Nederlands reisdocument wordt geprobeerd de best mogelijke vingerafdrukken op te nemen. Van een vinger wordt niet 1 opname gemaakt maar minstens 2. Zo wordt bij de aanvraag gecontroleerd of de vingerafdrukken kunnen worden geverifieerd.
>
> *Bij uitgifte vindt verificatie van de vingerafdrukken plaats indien de uitgevende instantie er aan twijfelt of de persoon die het reisdocument komt ophalen ook de persoon is die het reisdocument heeft aangevraagd.* De houder van een Nederlands reisdocument kan bij alle uitgevende instanties van de reisdocumenten inzage krijgen in de gegevens die over hem zowel in de chip als in de reisdocumentenadministratie zijn opgeslagen."[305]

De meest opvallende passage in deze brief betreft het 'verbod' op reguliere verificatie van de vingerafdrukken in de chip bij de uitgifte van elk reisdocument. Dit 'verbod' werd enkele dagen later als volgt bevestigd in een nadere instructie van agentschap BPR:

> "*Bij uitreiking van het reisdocument moeten de vingerafdrukken worden geverifieerd indien er sprake is van twijfel over de identiteit van de aanvrager.* Het kan voorkomen dat deze verificatie van de vingerafdruk mislukt. (...) Wanneer deze situatie zich voordoet kan de huidige procedure van retourdocumenten worden gevolgd. Dat wil zeggen dat als de verificatie van de vingerafdruk mislukt de afgevende instantie het reisdocument retour dient te sturen aan Sagem Identification (...). *Let wel: Het verifiëren van de vingerafdrukken bij de uitgifte van een reisdocument moet alleen plaatsvinden indien wordt getwijfeld of de persoon die het document komt ophalen ook de aanvrager van dat document is geweest.*"[306]

Dit terwijl in augustus 2008 nog door de staatssecretaris aan de Tweede Kamer was gemeld dat "bij uitgifte [van het reisdocument] verificatie van de vingerafdrukken [zal] plaatsvinden zodat kan worden vastgesteld dat de vingerafdrukken van de persoon aan wie het document wordt uitgereikt succesvol te verifiëren zijn tegen de opgenomen vingerafdrukken."[307] In de eerdere memorie van toelichting was de eventuele mogelijkheid om het reisdocument uit te geven door middel van toezending aan burgers per post om deze reden zelfs verworpen:

> "In de eerste plaats zou dit de verificatie van het reisdocument bij uitreiking onmogelijk maken. Er kan dan niet meer gecontroleerd worden of het document kan worden 'uitgelezen' en evenmin of de identiteit van degene die het reisdocument afhaalt, overeenkomt met degene die het reisdocument heeft aangevraagd (...)."[308]

In de brief van september 2009 werd tevens melding gemaakt van de overheidsfolder die diezelfde maand landelijk verspreid was. In de betreffende folder werd over de afname (en impliciet ook de opslag) van vingerafdrukken slechts vermeld dat dit zou voortvloeien uit een Europese verordening met als doel om "misbruik van reisdocumenten zoveel mogelijk tegen te gaan."[309] Over de andere (waaronder strafrechtelijke) doelen van de nieuwe Paspoortwet werd in de folder met geen woord gerept. Ook werden burgers in de folder niet gewezen op hun (internationale, Europese en nationale) recht van inzage en eventuele correctie (laat staan bezwaar tegen opslag) van hun biometrische gegevens in de paspoortchip en in de reisdocumentenadministratie. Wel werd in de folder vermeld dat de controle van de vingerafdrukken bij de opname ervan mede "bedoeld [is] om na te gaan of geprobeerd wordt de eigen vinger af te dekken."[310] Op de (ook in de folder) genoemde website (www.paspoortinformatie.nl) leest de internetvaardige burger tenslotte echter dat "[t]egen de opslag van uw vingerafdrukken in de reisdocumentenadministratie geen bezwaar [kan] worden gemaakt, omdat hier sprake is van een wettelijk voorschrift waarvan niet kan worden afgeweken. Hetzelfde geldt bijvoorbeeld ook voor het opslaan van uw gezichtsopname (foto) in de reisdocumentenadministratie."[311] Zo werd de gemiddelde burger niet alleen nauwelijks geïnformeerd, maar wordt deze ook ontmoedigd om de mogelijkheden van bezwaar en beroep te hanteren die hem of haar rechtens ter beschikking (behoren te) staan.

Verdere brieven, Kamervragen en verkiezingsprogramma's

Een eerste evaluatie van de invoering van vingerafdrukken in reisdocumenten werd op 17 maart 2010 door de staatssecretaris aan de Tweede Kamer verstuurd. Hierin werd onder andere ingegaan op de (technische) opleiding van gemeentebaliepersoneel, nieuwe apparatuur en het (problematisch gebleken) opnemen van vingerafdrukken bij ouderen. Ook was er een passage over de behandeling van bezwaren van burgers:

> "Sinds de invoering van de vingerafdrukken heeft een aantal burgers bij gemeenten bezwaar aangetekend tegen het opnemen van de vingerafdrukken en/of het opslaan van de vingerafdrukken in de decentrale reisdocumentenadministratie. De gemeenten zijn, als uitgevende instantie, verantwoordelijk voor het behandelen van deze bezwaren."[312]

In tegenstelling tot de informatie op www.paspoortinformatie.nl leek dit te impliceren dat burgers wel degelijk bezwaar tegen een en ander zouden kunnen maken en dat die bezwaren ook (door de verantwoordelijke gemeenten) als zodanig dienden te worden behandeld. Verder werd naar aanleiding van enkele nieuwe zwakheden in de RFID-chips door de staatssecretaris erkend dat "garanties voor de toekomst op basis van uitkomsten van testen

uit het verleden feitelijk niet [zijn] te geven. Alle landen die elektronische reisdocumenten uitgeven zullen, in de 'rat race' tegen misbruik/fraude van de reisdocumenten (en de daarin opgeslagen gegevens), deze realiteit moeten accepteren."[313]

Naar aanleiding van kritische berichtgeving in de media[314] werden in maart 2010 door de SP en VVD een aantal Kamervragen gesteld.[315] Deze vragen hadden voornamelijk betrekking op het beheer van de biometrische gegevens in het (decentrale, gemeentelijke) Reisdocumenten Aanvraag en Archief Station (RAAS) door het (Franse, commerciële) bedrijf Sagem Identification, evenals de beveiliging van, toezicht op en toegang tot een en ander, het foutenpercentage bij de afname (*enrolment*) van vingerafdrukken en het ontbreken van verificatie van de biometrische gegevens op de chip bij uitgifte van het reisdocument. Bij de beantwoording hiervan door de staatssecretaris kwam onder andere het recht op inzage van de burger in zijn opgeslagen vingerafdrukken aan de orde:

> "De burger kan of bij de uitgifte van het document of daarna in de gemeente waar het reisdocument is aangevraagd vragen om de vingerafdrukken uit te lezen die in de chip van het reisdocument zijn opgeslagen. De twee in de chip opgenomen vingerafdrukken worden dan op een scherm getoond. Tevens kan de burger bij de gemeente waar hij zijn reisdocument heeft aangevraagd vragen om een afschrift van de gegevens die zijn opgeslagen in de decentrale reisdocumentenadministratie. In dat geval wordt een print gemaakt van die gegevens, inclusief de vier opgenomen vingerafdrukken."[316]

Voor nadere beschouwing hiervan alsmede van andere technische, industriële en opleidingsaspecten wordt de lezer echter verwezen naar een parallel 'black box'-onderzoek van de WRR.[317]

Tenslotte hebben een aantal politieke partijen het biometrische paspoort en de opslag van vingerafdrukken in negatieve zin opgenomen in hun verkiezingsprogramma's van 2010:

> D66 "wil de opslag van vingerafdrukken die verkregen worden bij de aanvraag van een nieuw paspoort beëindigen. Dit is een vorm van onnodige inbreuk van het recht op privacy van de burgers. Tevens weten we nooit waarvoor die vingerafdrukken in de toekomst wellicht ooit gebruikt gaan worden."[318]

> GroenLinks: "Er komt geen landelijke vingerafdrukkendatabank. De overheid slaat vingerafdrukken en gezichtsscans van aanvragers van identiteitsdocumenten alleen op in de chip van dat document, conform de Europese verordening, zodat kan worden gecontroleerd of pas en persoon bij elkaar horen."[319]

> PvdD: "Het opnemen van vingerafdrukken in het paspoort en opname in de centrale database moet ongedaan gemaakt worden."[320]

> SP: "In Europees verband pleiten we voor afschaffing van de vingerafdruk in het paspoort. Die vingerafdrukken gaan we niet opslaan in een groot databestand."[321]

2.14 Intermezzo: *insiders* aan het woord

2.14.1 Biometrische aspecten: gezichtsherkenning

Alle geïnterviewden staan in het algemeen positief tegenover het gebruik van biometrie, maar erkennen tegelijkertijd de risico's ervan. Karakteristiek zijn in dit verband de woorden van Jan Grijpink:

> "Biometrie is op termijn onmisbaar. Ik denk dat het één van de belangrijkste pijlers wordt van de informatiesamenleving. Maar zonder andere informatie heb je niets aan een biometrisch kenmerk. Het is echter wél bruikbaar om iemand te 'framen'; je kunt iemand echt het leven onmogelijk maken."[322]

Wat de biometrische aspecten van het nieuwe paspoort betreft klonk tijdens de interviews echter met name kritiek op de lage resolutie van de gebruikte pasfoto. Jan Grijpink en Ruud van Munster stellen hierover respectievelijk het volgende:

> "Men heeft nooit overwogen om een hoge resolutie foto in het paspoort te zetten; ik vind dat een misser. Foto's met een hoge resolutie werken immers zelfs beter dan andere biometrie. Ik vermoed dat dat komt doordat veel landen niet zo rechtsstatelijk zijn als wij, en die landen hadden waarschijnlijk geen zin om mee te doen aan een stelsel dat de controles daadwerkelijk verbetert. Die landen vinden het dus prachtig dat die lage resolutie foto nu internationaal voorgeschreven is."[323]

> "Je kunt je dan afvragen hoe doeltreffend die technologie is, en of het de impact op je privacy rechtvaardigt. Daar zou je kritisch naar moeten kijken. Dat mis ik momenteel. Ik zie niemand daar bovenop zitten, niemand die zich bijvoorbeeld afvraagt of er binnen ICAO ruimte is om naar een hogere resolutie van gezichtsscans te gaan."[324]

Hier komt volgens Ron van Troost nog bij dat "het nu aan de burger zelf is om een pasfoto te laten maken en die bij de gemeente in te leveren voor de aanvraag van een nieuw paspoort. Eventueel zouden burgers hun eigen pasfoto's vooraf dus zelfs kunnen 'photo-shoppen'. (...) Het feit dat er destijds voor gekozen is om de foto voor de gelaatsscan door de vakfotografen in plaats van door gemeenten te laten maken, heeft met de lobby van de fotografie-branche te maken."[325] Ook gebeurt het volgens Van Troost nu nog vaak "dat mensen er pas bij de gemeentebalie achterkomen dat ze niet over de juiste pasfoto's beschikken. Die mensen moeten dan weer terug naar de fotograaf voor nieuwe pasfoto's."[326] Van Munster zegt: "Als expert op beeldbewerkingsgebied kan ik echt gruwelen van de kwaliteit van de huidige foto in het paspoort. Het is toch eigenlijk van de gekke: je gaat naar de fotograaf, je laat daar een digitale foto maken die op papier wordt afgedrukt, met die papieren pasfoto ga je naar het stadhuis, daar maakt men er een scan van, vervolgens wordt dat nog eens digitaal omgezet, en dat ga je dan als je referentiekader gebruiken om mensen te kunnen herkennen."[327] Arnout Ruifrok geeft in dit verband aan "een voorkeur te hebben voor het laten maken van paspoortfoto's op het gemeentehuis. Dit zou immers drie technische omzettingen schelen en biedt garanties qua integriteit, actualiteitsgehalte en biometrische bruikbaarheid. Bovendien

zou het weleens goedkoper kunnen zijn dan de relatief dure vakfotografen. Het maken van pasfoto's vormt echter wel een groot deel van [hun] omzet."[328]

2.14.2 Biometrische aspecten: vingerafdrukken

Het gebruik van vingerafdrukken brengt grote risico's met zich mee, aldus Jan Grijpink:

> "Vingerafdrukken zijn met name extra vervelend omdat ze relatief onveranderlijk zijn, en omdat je ze overal achterlaat. In dat opzicht is het dus vervelender als vingerafdrukken gecompromitteerd zijn, dan bij een irisscan. Het document zelf is eigenlijk veel gevaarlijker dan een databank. We raken per jaar 250.000 documenten kwijt, en daar staan in de toekomst dus allemaal biometrische gegevens op. Dat is écht gevaarlijk. Vaak vind je die documenten niet meer terug. Dat is de reden dat ik moeite heb met het biometrische paspoort. Ik vind het biometrische paspoort een vergissing."[329]

Ook is er volgens Grijpink sprake van een niveauvergissing of schaalfout:

> "Het [biometrische paspoort] is gebaseerd op het inzicht dat men iemand trefzeker kan herkennen aan zijn vingerafdruk. Dit in beginsel kleinschalige inzicht mag men niet zomaar doortrekken naar de nationale of internationale schaal van grensbewaking. Anders is het onzeker of het biometrische paspoort oplevert wat men ervan verwacht. Grootschalige stelsels werken in de praktijk immers anders dan kleinschalige. (...) Opschalen zonder nader onderzoek naar de risico's van de grootschalige situatie is dus eigenlijk riskant."[330]

Verder kan volgens Grijpink "[d]oor nabootsen of namaken van de vingerafdruk die op het paspoort staat iemand anders ongemerkt door de controle komen zonder dat naderhand kan worden nagegaan wie dat gedaan heeft."[331]

Overigens zouden het aantal en de resolutie van de huidige vingerafdrukken in het paspoort en de reisdocumentenadministratie te laag zijn om voor opsporingsdoeleinden te kunnen worden gebruikt, zo blijkt uit het interview bij vtsPN:

> "[V]oor forensische doeleinden [heeft men] niet veel aan de vier vingerafdrukken die voor het paspoort zijn afgenomen. Die vingerafdrukken zijn immers platte scans met een lage resolutie. Voor forensische doeleinden zijn gerolde vingers van 1000 dpi nodig. (...) Ik denk niet dat de KLPD er voor forensische doeleinden blij mee zal zijn; zij stellen daar hogere eisen aan."[332]

2.14.3 Een alternatief voor principieel bezwaarden?

Om de burger alsnog keuzevrijheid te kunnen bieden zijn er volgens Fons Knopjes wel alternatieven voor identificatie op nationaal niveau denkbaar:

> "[D]at betekent dat je de reisfunctie van de identiteitskaart af zou kunnen halen. We hebben nu in de Paspoortwet de identiteitskaart als een reisdocument gedefinieerd. Als we dat niet langer zouden doen en zouden zeggen 'nee, het is geen reisdocument, het is puur een identiteitsdocument', dan kun je de burger wél die keuzevrijheid bieden. We hebben de biometrie die erop staat immers als gevolg van de reisfunctie en internationale verplichtingen. Maar als je dus zegt: 'ik ga zo ver dat ik mijn burger wil kunnen laten kiezen', dan moet je een document in het leven roepen dat je alleen op nationaal niveau gebruikt en waarbij de burger

> kan kiezen voor wel of geen biometrie. En zo ver zijn we nooit gekomen. Nationaal is dat dus een optie, internationaal echter niet."[333]

2.14.4 Wel of geen (de)centrale opslag van biometrische gegevens?

Over de (modaliteiten van) opslag van biometrie bleken de meningen tijdens de interviews verdeeld. Aan de ene kant werd door Knopjes en Grijpink gesteld dat opslag in een database (in het algemeen) een goede Nederlandse keuze zou zijn.[334] Dit in tegenstelling tot bijvoorbeeld de Duitse situatie, waar een en ander alleen wordt opgeslagen in de chip van het document. "In Duitsland staan er alleen vingerafdrukken op het paspoort; de Duitse overheid mag zelfs geen kopie houden. Dat komt voort uit de privacylobby daar. Ze doen er momenteel verder niets mee en controleren de vingerafdrukken niet eens," vertelt Grijpink.[335] Opslag in een database zou volgens Knopjes echter effectiever zijn ter bestrijding van *look-alike* fraude en dubbele aanvragen. "Verificatie van de vingerafdruk via een database is daar een heel goed middel tegen. Zonder zo'n database heb je geen referentiemiddel."[336]

De keuze voor centrale in plaats van decentrale opslag zou volgens Knopjes voortvloeien uit de politieke ambitie van plaatsonafhankelijke aanvraag en uitgifte van reisdocumenten.[337] (Overigens zou dit argument oorspronkelijk van het CDA afkomstig zijn.[338]) Ook zou decentrale opslag met een centrale verwijsindex in technische en praktische zin (inclusief management) volgens hem te bewerkelijk zijn.[339] Knopjes: "Nog los van het beveiligings-issue, natuurlijk. Op één plek kun je de juiste maatregelen nemen om het goed te beveiligen. Het is een gegeven dat men op al die 700 plaatsen niet op hetzelfde, en misschien zelfs niet op het vereiste niveau van beveiliging zit. Nadeel is echter dat, als het bij centrale opslag fout gaat, het ook écht fout gaat."[340] En er zijn volgens Grijpink ook andere fundamentele risico's:

> "Biometrie is in wezen waarschijnlijkheidsberekening.(...) Elke biometrische meting is immers weer anders; geen enkele meting is 100% identiek. Dus hoe groter die databank, en hoe groter je doelgroep, hoe minder je ermee kunt, statistisch gezien."[341]

Bovendien bleken BZK en Justitie er in het verleden verschillende visies op te hebben nagehouden: zo zou vanuit BZK zijn gepleit voor decentrale opslag in de gemeentelijke databanken, en vanuit Justitie voor decentrale opslag met een centrale verwijsindex. Grijpink licht toe:

> "We wilden absoluut een databank. Sterker nog: als er twee vingers op het paspoort staan, wilden we vier vingers in een databank hebben. De eerste twee vingerafdrukken om te kunnen controleren of het paspoort authentiek is, en de andere twee om te kunnen controleren of het de juiste persoon is. Dat idee van vier vingerafdrukken was mijn idee. Om identiteitsfraude te kunnen bestrijden, moet je immers variatie in het proces kunnen aanbrengen. (...) Het betreft dan decentrale opslag met een centrale verwijsindex. Maar nu zijn we 5 jaar verder en hoor je opeens iedereen praten over een 'centrale databank'. Maar volgens mij kan dat helemaal niet. (...) De term 'centrale opslag' die in de huidige discussie zo'n overheersende rol dreigt te gaan spelen zie ik als een vergissing, of als een foute implementatie. (...) Een databank met de

> biometrische gegevens van 16 miljoen Nederlanders, dat zou statistisch gezien een puinhoop worden vanwege de duizenden 'near matches' die je dan krijgt. (...) Een nationale centrale databank lijkt me een onmaakbaar en onwerkbaar iets. (...) Een centrale databank zou een ramp kunnen worden. Na drie incidenten zou men het hele systeem platleggen. Zoiets kost dan alleen maar geld."[342]

Wel is er volgens Grijpink een centrale verwijsindex "nodig om ergens op terug te kunnen vallen als iemand zijn document kwijt is. (...) Biometrie brengt immers nieuwe vormen van identiteitsfraude met zich mee (...). Bewijs maar eens dat je bent wie je zegt dat je bent als iemand anders al op jouw naam maar met zijn eigen vingerafdrukken een paspoort heeft aangevraagd. Het is dus een riskante technologie als je vingerafdrukken op het paspoort hebt. Ik vind dat je die gemeentelijke databank nodig hebt om dit te kunnen 'tackelen' met inbegrip van een centrale index."[343] Hij acht een "systeem waarbij alle decentrale databanken via een centrale toegang tegelijk te doorzoeken zijn op één biometrische kenmerk [echter] een slecht, niet werkbaar concept, vooral door het eerdergenoemde statistische karakter van biometrie."[344]

Overigens ontstond er tijdens de interviews geen duidelijkheid over de exacte vorm die de Nederlandse centrale opslag zou gaan krijgen. Verder zou Nederland in toenemende mate uit de pas lopen bij de rest van Europa, zo bleek althans uit het interview bij het ministerie van Buitenlandse Zaken:

> "De geluiden die ons vanuit andere landen van Europa bereiken duiden juist op een tegengestelde beweging, dus richting decentrale opslag, ook vanuit veiligheidsoverwegingen."[345]

Tenslotte werd door Van Munster nog gesteld dat "aan grootschalige opslag van biometrie sowieso risico's zijn verbonden, hetzij doordat het denken over de toepassing ervan met de tijd verandert, hetzij in het geval van een totalitair regime."[346]

2.14.5 Gebrek aan verificatie en controle-infrastructuur

Sinds september 2009 worden aan alle burgers paspoorten met biometrische vingerafdrukken uitgegeven. Van technische verificatie van de biometrie op de chip bij uitgifte van het paspoort blijkt echter nauwelijks sprake. Van Troost licht toe:

> "Bij de uitgifte van het biometrische paspoort mogen de biometrische gegevens van de veronderstelde houder alléén door de gemeente worden geverifieerd in geval van twijfel over de identiteit van die persoon. Dit gebeurt dus niet standaard. (...) De gemeenten zelf waren eerder wel van mening dat de verificatie van biometrie bij de uitgifte van paspoorten een methode zou kunnen zijn om *look-alike* fraude te bestrijden. Maar bij de gemeenteloketten mogen de vingerafdrukken dus niet worden geverifieerd; dat mag alléén in twijfelgevallen. BPR heeft dat bepaald; dit is vlak voor de invoering van de vingerafdrukken op het paspoort door BPR gecommuniceerd aan alle gemeenten en aan de NVVB. BPR deed dit overigens zonder (kenbare) argumentatie. Een mogelijke reden zou kunnen bestaan uit de lastige situatie die

> zou kunnen optreden als zou blijken dat veel vingerafdrukken niet zouden kunnen worden geverifieerd."[347]

Ook bij het ministerie van Buitenlandse Zaken (BZ) is men bekend met deze instructie aan gemeenten, maar heeft men hier een eigen draai aan gegeven:

> "De keuze van wel of niet verifiëren is in principe juist aan de burger. Dus zeggen wij tegen de burger: 'laat u alstublieft uw vingerafdrukken bij ophalen van uw paspoort verifiëren, want dan weten wij zeker dat u correct in het document staat.' Bij twijfel over de identiteit van de afhaler heeft een ambtenaar inderdaad de *plicht* om die verificatie uit te voeren."[348]

Overigens werd bij BZ erkend dat het biometrische paspoort voor in het buitenland woonachtige Nederlanders een vermindering in dienstverlening tot gevolg kan hebben:

> "Voorheen konden reisdocumenten op alle locaties die aan BZ waren gelieerd worden aangevraagd: zo'n 500 buitenlandse kantoren. Door de investering in biometrie hebben we dat aantal moeten terugbrengen tot ongeveer 185. In een aantal gevallen moeten mensen daardoor verder reizen om een aanvraag te doen. De beleidskeuze voor biometrie heeft in die zin dus effect op de service die de burger kan verwachten van de overheid. (...) Veel andere Europese landen hebben die dienstverlening [overigens nog] veel verder teruggebracht. Sommigen Europese landen gaan zelfs zo ver dat je naar je land van herkomst terug moet om een nieuw paspoort te kunnen aanvragen."[349]

Daarnaast is er in het algemeen nog geen bijbehorende controle-infrastructuur ontwikkeld. Fons Knopjes geeft hierop het volgende commentaar:

> "[W]e kunnen op dit moment nergens die vingerafdruk uitlezen. Je kunt er nu dus eigenlijk niets mee; het loopt vooruit op toekomstige ontwikkelingen. Ik denk dat we minstens 5 jaar nodig hebben om die controle-infrastructuur goed van de grond te krijgen. Dat betekent dat je 5 jaar technologie aan boord hebt waar je niks mee doet. Dat beschouw ik als een vorm van kapitaalvernietiging. De vingerafdruk is dus te vroeg ingevoerd. Het creëert nu schijnveiligheid; de controle is immers niet veranderd. Op Schiphol loop je nog steeds gewoon langs de Koninklijke marechaussee; ze kunnen alleen je foto bekijken m.b.v. speciale paspoort-scanners. (...) Toekomstige gebruiksmogelijkheden voor de vingerafdruk, zoals bij E-overheidsdienstverlening en in de private sector, zijn nu nog totaal niet ontwikkeld."[350]

2.14.6 'Function creep'

Wat het onderwerp *function creep* betreft kan allereerst een algemene opmerking van Van Troost worden aangehaald:

> "Bij dit onderwerp gaat het niet zozeer alleen over het biometrische *paspoort*, maar over biometrische *reisdocumenten*, waaronder ook de NIK: de Nederlandse identiteitskaart. Verder is het verschil tussen *identificeren* en *legitimeren* belangrijk. Een reisdocument heeft enerzijds een *legitimerende* functie, namelijk voor internationale grenspassage. Anderzijds is een reisdocument veel breder inzetbaar, namelijk ter *identificatie* in allerlei situaties."[351]

Als belangrijkste actuele toepassing van het biometrische paspoort (en de NIK) werd door Van Munster 1:1 (gezichts)controle bij grenspassage genoemd.[352] De risico's van *function creep* en verschuivende opsporingsdoeleinden werden door hem echter bevestigd:

> "Met betrekking tot de centrale database is sprake van een glijdende schaal. In eerste instantie zou de database worden afgeschermd en alleen bestemd zijn voor *duplicate checks*; net als bij het RAAS. De doelstelling was slechts het checken van 1:1; het kunnen verifiëren of iemand de eigenaar is van een bepaald reisdocument. (...) Maar als het nu alleen in heel uitzonderlijke gevallen [ook strafvorderlijk] geraadpleegd mag worden, dan mag het over 10 jaar voor een winkeldiefstal."[353]

> "Het hele paspoortproject is volgens mij gericht op 1:1 [verificatie]. De 1:N [identificatie] is de *function creep* die gaat optreden als opsporingsdiensten meer gaan doen dan alleen de identiteit van een gevonden verdachte verifiëren. BPR heeft destijds duidelijk gesteld tegenover het NBF dat de toegang tot de database uitsluitend is bedoeld om de identiteit van een gevonden verdachte te kunnen controleren."[354]

In dit verband werd door Van Munster verder het belang van transparantie bij het gebruik door opsporingsdiensten benadrukt.[355] "De ontwikkeling van de techniek is in kwalitatieve zin niet tegen te houden. Het is dan ook van groot belang om misbruik te voorkomen door de relevante processen op orde te hebben. De techniek zelf is niet tegen te houden, maar er dient wel altijd heel goed te worden nagedacht over het gebruik ervan", aldus Van Munster.[356]

Volgens Grijpink zou het niet zozeer gaan om het opsporingsbelang van een biometrische database, aangezien de betreffende opsporingsbevoegdheden reeds zouden hebben bestaan:

> "Als er een verdenking is tegen iemand, mag de politie alles vorderen wat nodig is voor het onderzoek, waaronder de biometrie; dat RAAS/ORRA-systeem zit nu bij de gemeente. Die bevoegdheid heeft de politie op grond van het Wetboek van Strafvordering. Zodra er een verdenking is tegen een persoon, mogen gegevens over die persoon altijd opgevorderd worden; soms met toestemming van het OM, soms met toestemming of in opdracht van de rechter. Er is geen beperking. (...) Ik vind dan ook de angst van mensen voor een biometrische databank, dat zo'n databank gevaarlijk zou zijn voor de vrijheid van het individu tegenover de overheid, eigenlijk een beetje absurd. Die bevoegdheden bestaan immers al. Men zou bij wijze van spreken in een opsporingsonderzoek alsnog biometrie kunnen gaan verzamelen."[357]

Overigens had ook de NVVB eerder geadviseerd "dat naast automatische controle het voor opsporingsambtenaren mogelijk moeten [*sic*] zijn ook ad-hoc alle gegevens te kunnen raadplegen inclusief biometrie in het kader van misdaden waarvoor een straf hoger dan 4 jaar geldt (bijvoorbeeld bij terrorisme, georganiseerde misdaad etc.). Dit zou dan met toestemming van de Officier van Justitie kunnen."[358]

Verder zouden bezwaren over het feit dat de Paspoortwet nog grotendeels moest worden uitgewerkt in lagere wetgeving volgens Grijpink onterecht zijn:

> "Een AMvB wordt net zo zwaar doorgemeten als een wet. Daar wordt hier bij het wetgevingskwaliteitsbeleid van Justitie heel serieus naar gekeken. Het wordt bij het Parlement ter visie gelegd ('voorgehangen'); zij hebben er dus complete controle op. Als het Parlement erover wil praten, dan wordt erover gepraat."[359]

Over het toekomstige netwerk van gebruikers van de ORRA[360] merkt Knopjes het volgende op:

> "Ik zou me niet kunnen voorstellen dat BZK motieven heeft om identiteitsinformatie uit de database via het internet toegankelijk te maken voor een breed publiek. Wel kan ik me voorstellen dat documentnummers uit die database via het internet raadpleegbaar worden, hopelijk voor publieke en private partijen in binnen- en buitenland, zodat zij kunnen checken of een bepaald document is uitgegeven ('hit/no hit') en of er eventueel iets mee aan de hand is."[361]

Verder zou het biometrische paspoort volgens Knopjes niet geschikt zijn voor terrorismebestrijding:

> "Het is voor terrorismebestrijding niet het goede middel. Als je daar succesvol mee aan de slag wilt, moet je het gehéél managen. (...) Terroristen maken amper gebruik van valse paspoorten. Je komt het incidenteel tegen, maar dat staat niet in verhouding tot de grote investeringen die we doen. En dat in de wetenschap dat we op een aantal plaatsen in de wereld geen betrouwbare bevolkingsadministraties hebben en overheden geen beleid hebben als het gaat over identiteitsmanagement. Ook door die overheden worden identiteits- en reisdocumenten uitgegeven. Dat soort situaties kunnen een echte bedreiging voor ons vormen."[362]

In het kader van terrorismebestrijding gaat het ook volgens Ruifrok om "een zeer klein aantal mensen, die meestal ook gewoon authentieke reisdocumenten gebruiken."[363]

Wat de toegevoegde waarde van het biometrische paspoort en opslag van biometrie voor de wettelijke identificatieplicht en openbaar cameratoezicht betreft, zouden nu nog geen harde uitspraken kunnen worden gedaan. Qua toekomstige mogelijkheden zou bijvoorbeeld echter wel kunnen worden gedacht aan 'mobile identification', aldus Van Munster:

> "Opsporingsambtenaren zouden wellicht de beschikking kunnen krijgen over draagbare apparatuur waarmee een link gelegd kan worden tussen de chip in iemands paspoort en een centrale database. In technisch opzicht zal daar over een klein aantal jaren geen belemmering voor bestaan. Hetzelfde geldt in de latere toekomst wellicht ook voor openbaar cameratoezicht. De techniek voor gezichtsherkenning is momenteel nog lang niet zo ver, maar over een jaar of 15 misschien wel. De herkenning van een 'face in the crowd' wordt op dit moment nog beschouwd als een grote technologische uitdaging, althans voorzover bij TNO bekend."[364]

Door Ruifrok werd in dit verband opgemerkt dat de vingerafdruk in het paspoort behalve ter verificatie (1:1) waarschijnlijk ook zou kunnen gaan dienen ter *identificatie* van personen (1:N). Het feit dat dit nu nog niet gebeurt zou volgens hem vooral te maken hebben met een gebrek aan maatschappelijke acceptatie terzake.[365]

2.15 Tussenconclusie

Opvallend in de wetsgeschiedenis van het biometrische paspoort is allereerst het enorme verschil in gebruiksdoelen tussen het nooit in werking getreden wetsvoorstel van 2002 en de nieuwe Paspoortwet van 2009: terwijl in 2002 nog slechts sprake leek van *verificatie* van het reisdocument door middel van decentraal opgeslagen biometrie, werd in 2009 de wettelijke basis gelegd voor *identificatie* door middel van centraal opgeslagen biometrie voor

allerhande doeleinden, waaronder zelfs opsporing en vervolging. Zowel in 2002 als in 2009 was sprake van een negatief advies terzake van het CBP. De Raad van State adviseerde in 2002 positief en deed er in 2009 min of meer het zwijgen toe. Kritische Kamervragen waren in beide tijdvakken vooral afkomstig van de linkerzijde van het politieke spectrum. Gezien het summiere karakter van de parlementaire geschiedenis rond het voortijdig verouderde (en daarom ingetrokken) wetsvoorstel van 2002, zullen hieronder vooral de in dit onderzoek centraal staande beginselen de revue passeren voorzover zij een rol speelden bij de parlementaire behandeling van de nieuwe Paspoortwet van 2009.

Aan het beginsel *privacy* werd in de recente parlementaire geschiedenis weliswaar enige aandacht besteed, maar slechts door een klein aantal politieke partijen en van regeringszijde op relatief beperkte, eenzijdige wijze. Door de verantwoordelijke staatssecretaris werd in dit kader voornamelijk aangevoerd dat de nieuwe Paspoortwet geen grote veranderingen teweeg zou brengen in de reeds bestaande juridische situatie en dat *daarom* de privacy voldoende gewaarborgd zou zijn. (Overigens nam ook de PvdA dit standpunt in.) Weliswaar werd toegegeven dat zou worden overgeschakeld van papieren, decentrale en relatief beperkt toegankelijke (gemeentelijke) reisdocumentenadministraties naar een digitale, centrale en online raadpleegbare administratie waaruit voor meerdere doelen aan talloze partijen gegevens zouden kunnen worden verstrekt, en dat reeds daardoor in algemene zin sprake was van een inbreuk op de persoonlijke levenssfeer (zeker waar het de verwerking van biometrische gegevens zou betreffen). Die inbreuk zou echter worden gerechtvaardigd door de (beweerdelijk) legitieme doelen ervan, waaronder met name de bestrijding van identiteitsfraude c.q. *look-alike* fraude. Van enige cijfermatige onderbouwing hiervan was echter geen sprake; iets wat ook vanuit het oogpunt van *transparantie* en *efficiency* saillant genoemd mag worden. Bovendien was reeds eerder gebleken dat plaatsonafhankelijke aanvraag en uitgifte van reisdocumenten juist tot meer identiteitsfraude zou kunnen leiden. Naar deze kwesties werd door Kamerleden echter niet gevraagd. Een ander opvallend, veelgebruikt argument van regeringszijde is dat de (brede) doelen van gegevensverstrekking onder de nieuwe Paspoortwet nauwkeurig zouden zijn geformuleerd, en dat *daarom* geen sprake zou zijn van strijd met het recht op privacy. Met andere woorden: reeds de wettelijke ‘kenbaarheid’ van een en ander zou de mensenrechtelijke legitimiteit ervan creëren. In dit verband dient tevens te worden opgemerkt dat de zaak *Marper v. UK* (EHRM) van regeringszijde eenvoudigweg niet van toepassing werd geacht; dit vanwege een beweerdelijk gebrek aan strafrechtelijke context en het feit dat de nieuwe Paspoortwet de hele Nederlandse bevolking bestreek en dus niet tot stigmatisering van een bepaalde groep zou kunnen leiden. Verder werd de veiligheid van centrale opslag tegenover het parlement eenvoudigweg gesteld maar nimmer concreet onderbouwd, laat staan aangetoond. Hetzelfde geldt voor de risico’s

van *function creep*; zelfs het *bestaan* daarvan werd door de staatssecretaris *in casu* vrijwel geheel ontkend. (Uit diverse opmerkingen van het CDA, PVV en VVD bleek overigens dat dit risico juist zeer groot is. Zo pleitte de PVV voor openstelling van de gehele database ten behoeve van sporenonderzoek en liet het CDA blijken de database te willen gebruiken voor de bestrijding van *alle* misdrijven en overtredingen. De VVD reageerde hierop niet negatief.) Op al deze punten is door Kamerleden niet doorgevraagd. Evenmin lijkt men zich ooit te hebben afgevraagd of een centrale, online raadpleegbare database met de biometrische gegevens van 16 miljoen Nederlanders op termijn niet juist tot (veel) meer identiteitsfraude en andere problemen zou kunnen gaan leiden, hetzij van binnenuit (door corruptie of door datalekken), hetzij van buitenaf (*hacking*). Verder dient hier nog te worden opgemerkt dat, hoewel de staatssecretaris stellig ontkende dat de centrale database een opsporingsregister zou worden, dit niet zal kunnen voorkomen dat de database als zodanig zal kunnen worden *gebruikt*. Hetzelfde geldt voor haar ontkenning met betrekking tot *datamining* (bijvoorbeeld door veiligheids- en inlichtingendiensten). Tenslotte dient hier nog te worden opgemerkt dat in de parlementaire discussies geen aandacht werd besteed aan mogelijke (toekomstige) risico's van de centrale opslag van biometrische gezichtsscans, waaronder *ethnic profiling*, discriminatie en koppeling aan cameratoezicht. Hetzelfde geldt voor de risico's van de gebruikte RFID-technologie.

Tijdens de interviews verschilden de meningen over de vraag of de opslag van biometrie centraal of decentraal (met een centrale verwijsindex) zou moeten plaatsvinden; hierbij werden van beide zijden zowel technische als praktische argumenten en veiligheidsoverwegingen genoemd. Tegelijkertijd zou in de rest van Europa in toenemende mate sprake zijn van decentrale opslag om veiligheidsredenen. Verder werd het risico van *function creep* erkend, maar leek men zelf reeds weinig moeite te hebben met het gebruik van een en ander voor opsporingsdoeleinden. Toekomstige gebruiksdoelen als mobiele identificatie en geautomatiseerd cameratoezicht zouden in technische zin slechts een kwestie van tijd (weliswaar jaren) zijn. Verder werd het feit dat de nieuwe Paspoortwet nog grotendeels moest worden uitgewerkt in lagere wetgeving door de geïnterviewden niet als een probleem gezien.

Wat het beginsel *keuzevrijheid* voor de burger betreft kan evenals in vorige tussenconclusies worden opgemerkt dat daar door de regering geen enkele waarde aan werd (en wordt) gehecht. Hoewel enkele parlementariërs de kwestie van principieel bezwaarden nadrukkelijk aan de orde stelden, bleef het antwoord van de staatssecretaris steevast dat de Europese regelgeving hiertoe geen ruimte zou bieden en dat dergelijke keuzevrijheid ook niet wenselijk zou zijn, aangezien het een effectieve bestrijding van identiteitsfraude zou bemoeilijken.

“Geen vingerafdrukken, geen paspoort”, zo luidt het devies. Juridisch bezwaar daartegen zou volgens BZK niet mogelijk zijn. De *identiteit* van principieel bezwaarden wordt hierdoor als het ware dubbel ontkend. In dit verband bleek de overheid er overigens wel rekening mee te houden dat sommigen voor het aanvragen van een nieuw reisdocument misschien hun vingertoppen zouden proberen af te dekken of te verwonden.

Qua *keuzevrijheid* voor de overheid is tegelijkertijd duidelijk dat Nederland zelf heeft gekozen voor (centrale in plaats van decentrale) opslag van biometrie; hiertoe was men onder de Europese paspoortverordening geenszins verplicht. Verder was er voor het parlement wellicht sprake van enig gebrek aan keuzevrijheid vanwege het feit dat de nieuwe Paspoortwet een zogenaamde ‘nationale kop’ op diezelfde Europese verordening vormde. Het parlement werd hierdoor als het ware voor het blok gezet om deze (voor menig Kamerlid ondoorzichtige) mix van Europese en nationale wetgeving als ‘package deal’ te aanvaarden.

Om de burger alsnog enige *keuzevrijheid* te kunnen bieden werd tijdens de interviews het idee van een nationaal identiteitsdocument zonder biometrie geopperd. (Wegens internationale verplichtingen zou dit document echter niet als reisdocument kunnen worden gebruikt.) Een dergelijk document voor binnenlands gebruik zou ook een vorm van erkenning zijn voor de *identiteit* van principieel bezwaarden.

Opvallend in de wetsgeschiedenis is in het algemeen het enorme gebrek aan *transparantie.* Hoewel er enerzijds sprake is van regeling van diverse zaken op het niveau van formele wetgeving en AMv(R)B’s in plaats van bij ministeriële regelingen (wat dus in wezen meer transparantie schept), is anderzijds sprake van volstrekte onduidelijkheid over diezelfde nadere (toekomstige) regelingen onder het niveau van de wet in formele zin. Aldus tast men vooralsnog in het duister over tal van cruciale zaken. Bovendien bleek de staatssecretaris niet bij voorbaat voornemens om het parlement middels zogenaamde ‘voorhangprocedures’ te betrekken bij de latere opstelling van de betreffende AMv(R)B’s. Eenzelfde onduidelijkheid geldt eveneens nog altijd voor veel onderliggende (grotendeels niet openbaar gemaakte) studies, rapporten en onderzoeken van met name BZK en agentschap BPR; dit onderliggende materiaal komt in de parlementaire stukken en debatten vrijwel niet aan bod en is evenmin aan de orde gesteld. Tevens blijft in de parlementaire geschiedenis volstrekt onhelder welke binnen- en buitenlandse partijen bij een en ander betrokken zijn en wat hun belangen daarbij zijn. Door Kamerleden is ook hier niet naar gevraagd. Ook over het beheer en de beheerder(s) van de toekomstige centrale reisdocumentenadministratie werd slechts een enkele (onbeantwoorde) vraag gesteld (door D66). Enkele hoofddoelen van de nieuwe Paspoortwet zijn in de parlementaire behandeling zelfs vrijwel onbehandeld gelaten, waaronder de

binnen- en buitenlandse staatsveiligheid, terrorismebestrijding, rampenbestrijding en de uitvoering van wettelijke identificatieplichten. Bovendien werd de Nederlandse bevolking (na aanname van de wet) middels een folder van BZK op dusdanig onvolledige wijze ingelicht dat men welhaast zou kunnen spreken van misleiding. Van alle beginselen (op keuzevrijheid na) lijkt transparantie in dit dossier dan ook op de meest gebrekkige wijze te zijn ingevuld.

In het kader van *effectiviteit* en *efficiëntie* kan allereerst worden herhaald dat het primaire doel van de nieuwe Paspoortwet de bestrijding van identiteitsfraude zou zijn. Dit terwijl de door deze wet ingevoerde plaatsonafhankelijke aanvraag en uitgifte van reisdocumenten juist tot meer identiteitsfraude zou kunnen gaan leiden en *look-alike* fraude met Nederlandse reisdocumenten tot nu toe slechts een relatief kleinschalig fenomeen blijkt te zijn. Opvallend in dit verband is overigens dat uit de memorie van toelichting bij de nieuwe Paspoortwet blijkt dat er zou zijn gekozen voor de opslag van vier in plaats van twee vingerafdrukken ter verhoging van de slagingskans bij verificatie (het foutenpercentage was voorheen immers zo'n 3 procent). Tijdens de interviews bleek echter dat de opslag van deze twee extra vingerafdrukken (buiten het reisdocument) vooral was bedoeld als extra zekerheid voor de documenthouder tegen identiteitsfraude. Bovendien blijkt sinds de inwerkingtreding van de nieuwe Paspoortwet in het algemeen amper sprake te zijn van verificatie van de vingerafdrukken bij uitgifte van het reisdocument.

Wat de beginselen *effectiviteit* en *efficiëntie* betreft, bleek uit de interviews verder een gedeelde kritiek op de lage resolutie van de huidige gezichtsscan. Hetzelfde werd gezegd over de vingerafdrukken; de huidige kwaliteit daarvan zou voor opsporingsdoeleinden ongeschikt zijn. Tegelijkertijd leek men niet stil te staan bij de (nog) grotere inbreuk die een hogere kwaliteit van gezichtsscans en vingerafdrukken zou kunnen maken op de *privacy* van burgers, bijvoorbeeld door het grotere aantal (deels toekomstige) toepassingsmogelijkheden, waaronder ter opsporing en vervolging, identificatie en automatische herkenning door openbaar cameratoezicht. Aan de andere kant klonk er tijdens de interviews echter ook kritiek op het feit dat er überhaupt voor gekozen was om vingerafdrukken verplicht op te nemen in het paspoort; dit zou het paspoort juist gevoelig maken voor identiteitsfraude door kwaadwillenden. Verder klonk er kritiek op het feit dat de vingerafdruk in het paspoort was ingevoerd zonder tegelijkertijd een bijbehorende controle-infrastructuur te ontwikkelen, zowel bij internationale grenspassage als in het kader van de uitvoering van wettelijke identificatieplichten. Ook hierbij werd echter niet stilgestaan bij de grotere inbreuk op de privacy die een dergelijke infrastructuur teweeg zou (kunnen gaan) brengen. Tenslotte werd nog opgemerkt dat het biometrische paspoort geen effectief middel is voor

terrorismebestrijding, al is het maar vanwege het feit dat terroristen over het algemeen authentieke reisdocumenten gebruiken.

Van regeringszijde is tijdens de parlementaire behandeling nauwelijks ingegaan op de risico's van eventueel misbruik, onjuist en onvoorzien gebruik en de technische onvolkomenheden die inherent zijn aan grootschalige toepassing van biometrie. Ook bleek de staatssecretaris geen idee te hebben over actuele foutmarges. Verder kon de regering geen antwoord geven op de vraag of centrale opslag veiliger zou zijn dan decentrale opslag en werd de kwestie van overheidsaansprakelijkheid bij een eventuele *data breach* of biometrische identiteitsfraude bewust onbeantwoord gelaten. Van enige vorm van *accountability* vooraf is in die zin dan ook geen sprake. Dit geldt in het bijzonder voor concrete rechtsbescherming voor de burger bij biometrische identiteitsfraude. Verder werd een belangenafweging tussen centrale of decentrale opslag (met centrale verwijsindex) pas na forse kritiek terzake van het CBP opgenomen in de memorie van toelichting bij de nieuwe Paspoortwet. Vrijwel alle overige kritiek van het CBP en vergelijkbare negatieve adviezen van Nederlandse en Europese experts en toezichthouders werden structureel genegeerd of gebagatelliseerd. Aan de andere kant werd echter wel erkend dat biometrische identiteitsfraude iemand zijn leven lang kan blijven achtervolgen en onherstelbare schade teweeg kan brengen. De aanname van de Paspoortwet leidde vervolgens alsnog tot maatschappelijk en juridisch verzet, waarover meer in het volgende hoofdstuk.

Noten

1 Twee projectorganisaties waren met deze haalbaarheidsstudies belast.

2 Zie de brief van de minister voor Grote Steden- en Integratiebeleid (Roger van Boxtel) d.d. 3 juli 2002, *Kamerstukken II*, 2001-2002, 25764, nr. 19, p. 4.

3 Zie het wetsvoorstel tot wijziging van de Paspoortwet, onder andere in verband met het toepassen van biometrie in reisdocumenten, *Kamerstukken II*, 2001-2002, 28342, nrs. 1-4.

4 *European Conference for Issuing Authorities of Travel Documents: Exploring the use of Biometrics in Travel Documents* (20-21 juni 2002, Den Haag). Organisatie en leiding van de conferentie waren in handen van agentschap BPR.

5 Zie de brief van minister Van Boxtel d.d. 3 juli 2002, *supra* noot 2, pp. 2-3.

6 Ibid., p. 4.

7 Destijds werd in VWP-kader door de VS echter nog "geen verband gelegd met reisdocumenten"; zie *Kamerstukken I*, 1987-1988, 20200V, nr. 150d, p. 16. Zie ook ibid., p. 15. Recente Nederlandse overheidsinformatie over het VWP luidt als volgt: "Vanaf eind jaren '80 neemt Nederland deel aan het [VWP] van de Verenigde Staten. Het visumbeleid van de VS wordt door dat land zelf vastgesteld en bekendgemaakt; daarover heeft de Nederlandse overheid geen zeggenschap. Een besluit van de Nederlandse overheid, of instemming van het Nederlandse parlement, is voor de effectuering van het visumbeleid van een ander land niet vereist. Voor nieuwe EU-lidstaten die tot het VWP zijn toegelaten dan wel toegelaten willen worden, is de opzet door de Verenigde Staten inmiddels anders gestructureerd. De basis is een *Memorandum of Understanding* (MoU). Daaraan wordt een tweetal overeenkomsten gekoppeld, gericht op uitwisseling van informatie ter voorkoming van terrorisme en de preventie en bestrijding van ernstige criminaliteit. Voor landen die al in het VWP waren opgenomen, [waaronder] Nederland, is het alsnog overeenkomen van een dergelijk MoU niet vereist. *Wel wil de Verenigde Staten op termijn met deze landen overeenkomsten sluiten, gericht op uitwisseling van informatie ter voorkoming van terrorisme en de preventie en bestrijding van ernstige criminaliteit. Nederland heeft op dit moment geen dergelijke overeenkomsten met de VS gesloten. Indien dit in de toekomst aan de orde zou zijn, zal het gebruikelijke traject voor parlementaire goedkeuring in acht worden genomen.*" Email van Peter Potman (Plaatsvervangend Directeur Westelijk Halfrond), ministerie van Buitenlandse Zaken, 16 maart 2010 (cursivering VB).

8 Zie de brief van minister Van Boxtel d.d. 3 juli 2002, *supra* noot 2, p. 3.

9 Zie bijvoorbeeld US Department of State, *The US Electronic Passport: Frequently Asked Questions*, http://travel.state.gov/passport/passport_2788.html.

10 Zie de brief van minister Van Boxtel d.d. 3 juli 2002, *supra* noot 2, p. 4; brief van minister De Graaf d.d. 19 december 2003, *infra* noot 34, p. 3; jaarverslag van BZK over 2003 (VII) d.d. 19 mei 2004, *Kamerstukken II*, 2003-2004, 29540, nr. 14, p. 117.

11 Onderzoeksrapport BPR 2003, *infra* noot 52, p. 25.

12 Zie de presentatie over het IF4TD van dhr. Sjef Broekhaar (BPR) tijdens het *Third Symposium on MRTDs, Biometrics and Security* (ICAO, Montréal, 1-3 oktober 2007), *slide* 8; beschikbaar op www.icao.int/mrtdsymposium/2007/Docs/W2_BroekhaarSjef.pdf.

13 Republic of Maldives, Department of Immigration and Emigration, *Immigration joins IF4TD (International Forum for Travel Documents)*, 13 november 2008; www.immigration.gov.mv/index.php/news/93-immigration-joins-if4td-international-forum-for-travel-documents.html.

14 Zie presentatie Broekhaar, *supra* noot 12, *slide* 12.

15 Email van Edmee Gosselink (BPR) aan de auteur d.d. 20 januari 2010 (hierna: email Gosselink).

16 Zie International Forum for Travel Documents, *Terms of Reference – version IF4TD/0.9/2007* (hierna: IF4TD TOR), p. 1. De participatie van de VN zou wellicht verklaard kunnen worden door de uitgifte van 'laisser-passers' aan VN-personeel en (door UNHCR) aan vluchtelingen en statenlozen. Hetzelfde zou voor het Rode Kruis kunnen gelden in verband met de uitgifte van speciale identiteitsdocumenten aan krijgsgevangenen, medisch en religieus personeel, oorlogscorrespondenten, personeel voor civiele bescherming en zelfstandige journalisten in oorlogsgebieden. Overigens zou biometrie voor het Rode Kruis verder wellicht van belang kunnen zijn ter opsporing van vermiste personen en ter identificatie van slachtoffers in rampgebieden. Navraag bij beide organisaties over hun rol en belangen bij participatie in het IF4TD leverde echter geen informatie op; bij relevante afdelingen van het Rode Kruis en UNHCR in Genève bleek men zelfs niet van het bestaan van het IF4TD op de hoogte.

17 Zie ibid., p. 3.

18 Email Gosselink, *supra* noot 15.

19 Ibid. Zie tevens IF4TD TOR, *supra* noot 16, p. 2.

20 Zie IF4TD TOR, *supra* noot 16, p. 2.

21 Zie ibid.

22 Email Gosselink, *supra* noot 15.

23 Email van Fons Knopjes (*managing director* van het ID Management Centre te Den Haag) aan de auteur d.d. 13 augustus 2010. (Zie over dhr. Knopjes tevens *supra*, tabel 1.1)

24 Zie ibid.

25 Zie bijvoorbeeld http://coolwhois.com/d/if4td.org/20100822180224 (geraadpleegd op 22 augustus 2010).

26 Zie email Gosselink, *supra* noot 15.

27 European Forum for Travel Documents, *Draft Terms of Reference and Guidelines for Participants* (januari 2003), p. 2.

28 Email Gosselink, *supra* noot 15.

29 Zie de brief van minister De Graaf d.d. 19 december 2003, *infra* noot 34, p. 3.

30 Zie het telegram van de Amerikaanse ambassade te Berlijn d.d. 3 juli 2003 aan het Amerikaanse ministerie van Buitenlandse Zaken naar aanleiding van de EFTD-conferentie te Berlijn d.d. 30 juni - 1 juli 2003, p. 5; beschikbaar op www.policylaundering.org/archives/ICAO/european_forum.pdf.

31 Ibid., pp. 1-6.

32 Zie met name de presentatie van dhr. Broekhaar *supra* noot 12. Zie tevens de vergelijkbare presentatie van Broekhaar tijdens het *Second Symposium on MRTDs, Biometrics and Security* (ICAO, Montréal, 6-8 september 2006); beschikbaar op www.icao.int/MRTDsymposium/2006/Docs.htm.

33 Zie ICAO, *Biometric Identification to provide enhanced security and speedier border clearance for travelling public*, PIO 09/03 (Montréal, 28 mei 2003).

34 Zie de brief van de minister voor Bestuurlijke Vernieuwing (Thom de Graaf) d.d. 19 december 2003, *Kamerstukken II*, 2003-2004, 25764, nr. 22, p. 2.

35 Zie paragraaf 2.6 *infra*.

36 Zie de brief van minister De Graaf d.d. 19 december 2003, *supra* noot 34, p. 3.

37 Ibid.

38 Zie ibid., p. 4.

39 WRR-interview Van Munster, *supra* tabel 1.1, p. 2.

40 WRR-interview Knopjes, *supra* tabel 1.1, p. 2.

41 Fons Knopjes in 'Biometrie: draak of geluksbrenger', Automatisering Gids, 8 mei 2003.

42 WRR-interview Van Troost, *supra* tabel 1.1, p. 3.

43 Zie bijvoorbeeld WRR-interview Van Munster, *supra* tabel 1.1, p. 3; WRR-interview Van Troost, *supra* tabel 1.1, p. 3 ; WRR-interview Knopjes, *supra* tabel 1.1, p. 4.

44 Zie Koninklijke Marechaussee, Expertise Centrum Identiteitsfraude en Documenten (ECID), *Statistisch Jaaroverzicht Documentfraude 2009* (Schiphol, conceptversie april 2010), pp. 16-18, 27-28, 40, 42-43. Zie voor de betreffende optelsom WRR-interview Kooij & Levering, *supra* tabel 1.1, pp. 2-3. Kooij en Levering zijn de auteurs van het genoemde *Statistisch Jaaroverzicht Documentfraude 2009*.

45 Zie WRR-interview Kooij & Levering, *supra* tabel 1.1, p. 3.

46 Zie ibid., p. 1.

47 Zie ibid., p. 2.

48 Zie bijvoorbeeld WRR-interview Grijpink, *supra* tabel 1.1, p. 3.

49 Ibid., p. 2.

50 Zie WRR-interview Knopjes, *supra* tabel 1.1, p. 2; WRR-interview Grijpink, *supra* tabel 1.1, pp. 2, 4.

51 Zie WRR-interview Knopjes, *supra* tabel 1.1, pp. 2, 5.

52 Agentschap BPR (BZK), *Onderzoek naar de toepassing van biometrische kenmerken in Nederlandse reisdocumenten* (Den Haag, 6 juni 2003) (hierna: onderzoeksrapport BPR 2003).

53 Zie ibid., pp. 4, 12.

54 Zie ibid.

55 Ibid., p. 5. Zie tevens ibid., p. 14.

56 Ibid., p. 10.

57 Zie ibid.

58 Ibid.

59 Ibid., p. 11.

60 Zie ibid.

61 Ibid (cursivering VB).

62 Ibid.

63 Ibid. Zie tevens de brief van de minister voor Grote Steden- en Integratiebeleid (Roger van Boxtel) d.d. 31 januari 2002, *Kamerstukken II*, 2001-2002, 25764, nr. 18, p. 5.

64 Zie paragraaf 2.1.1 *supra*. Zie voor de parlementaire behandeling van dit wetsvoorstel paragraaf 2.12 *infra*.

65 Onderzoeksrapport BPR 2003, *supra* noot 52, p. 8.

66 Ibid., p. 9.

67 Ibid. Hierbij wordt verwezen naar het rapport *Mensensmokkel in beeld 2000 – 2001* (Informatie- en Analysecentrum Mensensmokkel & Landelijk Parket Rotterdam, najaar 2002) en naar de Britse *National Forgery Section Netherlands document exercise* d.d. 28 december 2002; zie ibid.

68 Zie onderzoeksrapport BPR 2003, *supra* noot 52, p. 9. Zie in dit verband ook het *Actieplan Terrorismebestrijding en Veiligheid* (bijlage bij kabinetsbrief d.d. 5 oktober 2001, kenmerk 5125137/501/RD), pp. 2-3.

69 Onderzoeksrapport BPR 2003, *supra* noot 52, p. 15 (cursivering VB). Zie voor het onderzoek in kwestie *Biometrics against look alike in the next generation travel documents* (VKA & TNO, 10 december 2002) (nog niet openbaar). Hierbij was tevens een in juni 2002 door TNO (in opdacht van BPR) uitgevoerde laboratoriumtest naar gelaatsherkenning bij 129 personen (onder wie 28 tweelingen) betrokken. Zie ook onderzoeksrapport BPR 2003, *supra* noot 52, p. 15, n. 4. Zie hierover tevens *infra*, paragraaf 2.7.

70 Zie onderzoeksrapport BPR 2003, *supra* noot 52, p. 15.

71 Zie het rapport *Marktconsultatie voor biometrie op Nederlandse reisdocumenten* (Montelbaan, 28 april 2003).

72 Zie Max Snijder, *WRR Case Studie: Black Box Biometrisch Paspoort* (nog te verschijnen).

73 Zie onderzoeksrapport BPR 2003, *supra* noot 52, pp. 17, 19.

74 Zie ibid., pp. 18-19.

75 Zie voor de parlementaire behandeling van dit wetsvoorstel paragraaf 2.12 *infra*.

76 Onderzoeksrapport BPR 2003, *supra* noot 52, pp. 18-19.

77 Zie ibid., p. 21. Zie ook de nota 'Misbruik en oneigenlijk gebruik op het gebied van belastingen, sociale zekerheid en subsidies' d.d. 19 april 2002, *Kamerstukken II*, 2001-2002, 17050, nr. 234, pp. 36, 39.

78 Zie onderzoeksrapport BPR 2003, *supra* noot 52, p. 22.

79 Ibid., p. 30.

80 Ibid., pp. 31-32 (cursivering VB).

81 Ibid., p. 39.

82 Zie ibid., p. 40.

83 Ibid., p. 46.

84 Zie bijvoorbeeld ibid., p. 24.

85 R.L. van Renesse, *Quick scan biometrie – alle mensen zijn ongelijk*, TNO rapport EIB-RPT-990069 (in opdracht van agentschap BPR), 29 oktober 1999 (nog niet openbaar).

86 WRR-interview Van Munster, *supra* tabel 1.1, p. 1.

87 *Biometrics against look alike in the next generation travel documents*, VKA & TNO (in opdracht van agentschap BPR), 10 december 2002 (nog niet openbaar). Zie ook *supra*, noot 69.

88 WRR-interview Van Munster, *supra* tabel 1.1, pp. 2-3.

89 Zie ook *supra*, noot 69.

90 WRR-interview Van Munster, *supra* tabel 1.1, p. 2.

91 TNO-rapport I&I-RPT-020036 (september 2002) (nog niet openbaar).

92 Zie WRR-interview Van Munster, *supra* tabel 1.1, p. 2.

93 Zie ibid., p. 3.

94 Zie bijvoorbeeld WRR-interview Knopjes, *supra* tabel 1.1, p. 7.

95 WRR-interview Van Troost, *supra* tabel 1.1, p. 2.

96 WRR-interview Van Munster, *supra* tabel 1.1, pp. 2, 4.

97 WRR-interview Provily & Van der Zanden, *supra* tabel 1.1, p. 10.

98 WRR-interview Grijpink, *supra* tabel 1.1, p. 5. Overigens had Grijpink reeds in juli 2004 ook gesproken over "niet sporende visies" tussen Justitie en BZK op het terrein van biometrie; zie Peter Mom, *Volgens Justitie werkt biometrie in paspoorten averechts*, Automatisering Gids 16 juli 2004 (nr. 29), pp. 10-11.

---

99 Zie de brief van minister De Graaf d.d. 19 december 2003, *supra* noot 34, p. 2.

100 Ibid., p. 2.

101 Zie ibid., p. 3. Zie tevens *supra*, paragraaf 2.2.2.

102 Council of Europe, European Committee on Legal Cooperation, Group of Specialists on Identity and Terrorism (CJ-S-IT), *Final Activity Report of the Group of Specialists on Identity and Terrorism*, CJ-S-IT (2004)16 (Straatsburg, 23 april 2004), pp. 17-18 (cursivering VB); beschikbaar (inclusief *follow-up*) op www.coe.int/t/e/legal_affairs/legal_co-operation/fight_against_terrorism/4_theme_files/Identity_Documents.

103 Zie *supra*, paragraaf 2.3.1.

104 Almere, Apeldoorn, Eindhoven, Groningen, Rotterdam en Utrecht.

105 Zie de brief van de minister voor Bestuurlijke Vernieuwing (Thom de Graaf) d.d. 5 oktober 2004, *Kamerstukken II*, 2004-2005, 25764, nr. 24, pp. 1-2.

106 Zie de brief van de staatssecretaris van Buitenlandse Zaken d.d. 15 april 2004, *Kamerstukken II*, 2003-2004, 22112, nr. 318, pp. 2-5.

107 Zie de brief van minister De Graaf d.d. 5 oktober 2004, *supra* noot 105, p. 2.

108 Zie de brief van de ministers van Justitie (Piet Hein Donner; CDA), Vreemdelingen en Integratie (Rita Verdonk; VVD) en Binnenlandse Zaken (Johan Remkes; VVD) d.d. 2 november 2004, *Kamerstukken II*, 2004-2005, 23490, nr. 344, pp. 1-3.

109 Zie ibid., pp. 3-4.

110 Vergelijk ook *Kamerstukken II*, 2004-2005, 23490, nr. 336 (22 september 2004), waaruit het vertrouwelijke karakter van een en ander blijkt.

111 Brief van de ministers van Justitie (Piet Hein Donner) en Binnenlandse Zaken (Johan Remkes) d.d. 24 januari 2005, *Kamerstukken II*, 2004-2005, 29754, nr. 5, pp. 1-2 (cursivering VB).

112 Zie ibid., p. 5.

113 Ibid., p. 7.

114 Ibid., pp. 9-10 (cursivering VB).

115 Zie bijvoorbeeld *CBP bestudeert plan opslag biometrische gegevens*, ANP, 17 februari 2005; *Vrees voor misbruik van scans*, BN/DeStem, 18 februari 2005. Zie ook *Kenmerken Nederlanders in databank*, Volkskrant, 24 februari 2006, *infra* noot 203.

116 Meldpunt Misbruik Identificatieplicht, *Geen chip in mijn paspoort of ID-kaart* (Utrecht, 2006), p. 5.

117 Brief van de minister voor Bestuurlijke Vernieuwing (Alexander Pechtold) d.d. 18 april 2005, *Kamerstukken II*, 2004-2005, 25764, nr. 26, p. 1.

118 Ibid., p. 5.

119 Ibid., pp. 5-6.

120 Brief van de Permanente Commissie van deskundigen in internationaal vreemdelingen-, vluchtelingen- en strafrecht (Commissie Meijers) aan de vaste commissie voor Binnenlandse Zaken en Koninkrijksrelaties van de Tweede Kamer (CM0603), 13 april 2006, pp. 1-2. Zie tevens de bijbehorende notitie (CM0605-I) van dezelfde datum en een eerdere notitie d.d. 20 november 2003 (CM03-13). Deze documenten zijn beschikbaar op www.commissie-meijers.nl/commissiemeijers/pagina.asp?pagnaam=commentaren.

121 Brief van de minister voor Bestuurlijke Vernieuwing (Atzo Nicolaï; VVD) d.d. 31 augustus 2006, *Kamerstukken II*, 2005-2006, 25764, nr. 30, p. 5.

122 Verordening (EG) Nr. 2252/2004 van de Raad van 13 december 2004.

123 Zie de brief van de minister voor Bestuurlijke Vernieuwing Pechtold d.d. 18 april 2005, *supra* noot 117, pp. 1-2.

124 Zie ibid., p. 3.

125 Zie *supra*, paragraaf 2.8.2.

126 Zie de brief van de minister voor Bestuurlijke Vernieuwing Pechtold d.d. 18 april 2005, *supra* noot 117, p. 4.

127 Zie ministerie van Binnenlandse Zaken, *Evaluatierapport Biometrieproef 2b or not 2b* (september 2005; als bijlage opgenomen bij *Kamerstukken II*, 2004-2005, 25764, nr. 27), p. 6.

128 Zie *supra*, noot 104.

129 Zie *Evaluatierapport Biometrieproef 2b or not 2b*, *supra* noot 127, pp. 6, 11. De betreffende folder is als Bijlage 8 bij het evaluatierapport aangehecht.

130 Zie ibid., p. 11.

131 Zie ibid.

132 Ibid., p. 12.

133 Zie ibid.

134 Zie ibid: vergelijk de getallen in Tabel 1 op p. 19 met de getallen op p. 14. (Uit de getallen op p. 14 blijkt dat opname van de gelaatsscan in 231 (217 + 14) gevallen (1,6% van het totaal van 14735 aanvragen) niet succesvol was. Slechts het overgebleven (succesvolle) aantal van 14504 aanvragen is opgenomen in Tabel 1 op p. 19.).

135 Zie ibid: Tabel 1 op p. 19 en pp. 14, 28. Bovendien bevat de verificatiegroep in Tabel 1 alleen de documenten waarbij de opname van zowel de gelaatsscan als beide vingerafdrukken gelukt was. Zie ibid: vergelijk de getallen in Tabel 1 op p. 19 met de getallen op p. 14.

136 Zie ibid., p. 19 (inclusief Tabel 1). Zie tevens p. 29.

137 Zie ibid., p. 21, Tabellen 2-3.

138 Zie ibid., p. 17.

139 Zie ibid., p. 20.

140 Zie ibid., p. 26. Zie tevens ibid., p. 53 (Bijlage 5).

141 Zie ibid., pp. 28-30.

142 Ibid., p. 24.

143 Ibid., p. 26. Zie tevens ibid., Bijlage 6 (Rapport TNO).

144 Brief van de minister voor Bestuurlijke Vernieuwing Pechtold d.d. 12 september 2005, *Kamerstukken II*, 2004-2005, 25764, nr. 27, p. 2.

145 Ibid., p. 3.

146 Ibid.

147 Dit ondanks relatief brede aandacht voor de biometrieproef in de pers; zie bijvoorbeeld *Paspoort; het nieuwe identificeren*, Elsevier, 7 augustus 2004; *Een paspoort vol vingerafdrukken*, Financieel Dagblad, 21 augustus 2004; *Op zoek naar 15.000 vrijwilligers*, Parool, 30 augustus 2004; *Proef met nieuw paspoort*, Trouw, 31 augustus 2004; *Bent u het wel of bent u het niet?; biometrisch paspoort*, Vrij Nederland, 29 januari 2005.

148 WRR-interview Van Munster, *supra* tabel 1.1, p. 2.

149 WRR-interview Grijpink, *supra* tabel 1.1, p. 4.

150 WRR-interview Knopjes, *supra* tabel 1.1, pp. 2, 7.

151 Ibid., pp. 7-8.

152 WRR-interview Ruifrok, *supra* tabel 1.1, p. 4.

153 Ibid., p. 3.

154 Ibid.

155 Ibid.

156 Zie het wetsvoorstel tot wijziging van de Paspoortwet, onder andere in verband met het toepassen van biometrie in reisdocumenten (april 2002), *Kamerstukken II*, 2001-2002, 28342, nrs. 1-2.

157 Zie Advies Raad van State en Nader Rapport, *Kamerstukken II*, 2001-2002, 28342, A.

158 Advies College bescherming persoonsgegevens d.d. 16 oktober 2001 inzake wijziging Paspoortwet (invoering biometrie) (hierna: Advies CBP 2001), p. 4 (cursivering VB); beschikbaar op www.cbpweb.nl/Pages/adv_z2001-1368.aspx.

159 Zie memorie van toelichting bij het wetsvoorstel tot wijziging van de Paspoortwet, onder andere in verband met het toepassen van biometrie in reisdocumenten, *Kamerstukken II*, 2001-2002, 28342, nr. 3, p. 1, n. 1.

160 Zie het verslag van de vaste commissie voor Binnenlandse Zaken, *Kamerstukken II*, 2001-2002, 28342, nr. 5.

161 Zie Advies CBP 2001, *supra* noot 158, pp. 2, 4.

162 Zie verslag *supra* noot 160, p. 2.

163 Zie ibid. Zie tevens het rapport *At face value*, *supra* p. 29, noot 27, p. 69.

164 Zie verslag *supra* noot 160, pp. 3-4.

165 Ibid., p. 5.

166 Ibid.

167 Memorie van toelichting bij het wetsvoorstel ter wijziging van de Paspoortwet in verband met het herinrichten van de reisdocumentenadministratie, *infra* noot 173, p. 4.

168 Zie de brief van de minister voor Bestuurlijke Vernieuwing Pechtold d.d. 18 april 2005, *supra* noot 117, p. 4.

169 Zie ibid.

170 Zie de brief van de staatssecretaris van Binnenlandse Zaken (Ank Bijleveld-Schouten) d.d. 26 februari 2008, *Kamerstukken II*, 2007-2008, 28342, nr. 6.

[171] Zie het voorstel van rijkswet tot wijziging van de Paspoortwet in verband met het herinrichten van de reisdocumentenadministratie (januari 2008), *Kamerstukken II*, 2007-2008, 31324, nr. 2.

[172] Zie ibid., ingediend door de staatssecretaris van Binnenlandse Zaken (Ank Bijleveld-Schouten) op 21 januari 2008.

[173] Zie de memorie van toelichting (MvT) bij het voorstel van rijkswet tot wijziging van de Paspoortwet in verband met het herinrichten van de reisdocumentenadministratie, *Kamerstukken II*, 2007-2008, 31324, nr. 3, p. 2.

[174] Zie ibid.

[175] Zie ibid.

[176] Ibid., pp. 12-13.

[177] Zie ibid., p. 39.

[178] Ibid., p. 13.

[179] Zie ibid., pp. 6-7, 23.

[180] Ibid., p. 13.

[181] Zie ibid., p. 14. Zie over de biometrieproef '2b or not 2b' paragraaf 2.9 *supra*.

[182] Ibid., p. 18.

[183] Ibid.

[184] Advies College bescherming persoonsgegevens d.d. 30 maart 2007 inzake wijziging Paspoortwet in verband met de herinrichting van de reisdocumentenadministratie (hierna: Advies CBP 2007), pp. 8-9 (cursivering VB); beschikbaar op www.cbpweb.nl/Pages/adv_z2007-00010.aspx.

[185] Zie MvT, *supra* noot 173, par. 3.2. Zie tevens ibid., pp. 21-22.

[186] Ibid., p. 27. Zie tevens ibid., p. 12.

[187] Zie ibid., p. 28.

[188] Vergelijk bijvoorbeeld ibid., p. 23.

[189] Ibid.

[190] Zie ibid., p. 1.

[191] Verslag van de vaste commissie voor Binnenlandse Zaken d.d. 25 maart 2008, *Kamerstukken II*, 2007-2008, 31324, nr. 4.

[192] Zie ibid., pp. 2-3.

[193] Nota van staatssecretaris van Binnenlandse Zaken (Ank Bijleveld-Schouten) d.d. 16 juli 2008 naar aanleiding van het verslag, *Kamerstukken II*, 2007-2008, 31324, nr. 5, p. 3.

[194] Zie ibid., p. 6.

[195] Brief van de minister voor Bestuurlijke Vernieuwing (Atzo Nicolaï) d.d. 22 september 2006, *Kamerstukken II*, 2006-2007, 29515, nr. 157, p. 1. Zie voor het betreffende onderzoeksrapport ECORYS Nederland BV, *Plaatsonafhankelijke dienstverlening. Een stap vooruit?* (Rotterdam, april 2006), pp. 26-29, 31. (Dit rapport is als bijlage opgenomen bij bovengenoemde brief van minister Nicolaï d.d. 22 september 2006.)

[196] De Artikel 29-werkgroep is het onafhankelijke advies- en overlegorgaan van de Europese privacytoezichthouders. De werkgroep adviseert onder andere de Europese Commissie bij de totstandkoming van Europees beleid op het gebied van de bescherming van persoonsgegevens. De huidige voorzitter van de werkgroep is (CBP-voorzitter) Jacob Kohnstamm.

[197] Advies van de Europese Toezichthouder voor gegevensbescherming (Peter Hustinx) d.d. 26 maart 2008 (2008/C 200/01, 6.8.2008), par. 27-28 (cursivering VB); beschikbaar op www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2008/08-03-26_Biometrics_passports_NL.pdf. Peter Hustinx was voorheen overigens voorzitter van het CBP.

[198] Advies van de Groep gegevensbescherming artikel 29 d.d. 30 september 2005 (1710/05/NL - WP 112 - 04/09/12), par. 2.3(a); zie http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2005_en.htm.

[199] Zie de nota van staatssecretaris Bijleveld d.d. 16 juli 2008, *supra* noot 193, p. 8.

[200] Zie ibid., pp. 9-10.

[201] Zie ibid., p. 10.

[202] Ibid. Daarnaast zouden "de decentrale reisdocumentenadministraties in werking blijven totdat de nieuwe administratie is gevormd, getest en is aangetoond dat het werkt." Ibid.

[203] *Kenmerken Nederlanders in databank*, Volkskrant, 24 februari 2006, p. 1 (auteur: Michael Persson); beschikbaar op www.volkskrant.nl/binnenland/article229553.ece.

[204] Nota van staatssecretaris Bijleveld d.d. 16 juli 2008, *supra* noot 193, p. 11, met verwijzing naar een eerder jaarverslag van de AIVD over 2002.

[205] Ibid., p. 13.

[206] Ibid., p. 14.

[207] Ibid., p. 17.

[208] Ibid., p. 18.

[209] Ibid., p. 19.

[210] Ibid., pp. 20-21.

[211] Zie Rathenau Instituut, *RFID-bewustzijn van consumenten: hoe denken Nederlanders over Radio Frequency Identification?* (Den Haag, 2007), pp. 6, 31-34; beschikbaar op www.rathenau.nl/publicaties/rfid-bewustzijn-van-consumenten.html.

[212] Nota van staatssecretaris Bijleveld d.d. 16 juli 2008, *supra* noot 193, p. 26. Op de dag dat de nieuwe Paspoortwet voor alle burgers in werking trad sprak CBP-voorzitter Jacob Kohnstamm zich er echter nogmaals in negatieve zin over uit; zie telefonisch interview met Kohnstamm op BNR Nieuwsradio d.d. 21 september 2009, beschikbaar op www.bnr.nl/artikel/13173896/voortaan-vingerafdrukken-paspoort.

[213] Zie behandeling herinrichten reisdocumentenadministratie, *Handelingen II*, 2008-2009, TK 24, 2002-2003, 2008, 2009 (13 november 2008).

[214] Ibid., 2004 (lid Heijnen, PvdA; cursivering VB).

[215] Ibid., 2005 (lid Pechtold, D66; cursivering VB).

[216] Ibid., 2007 (lid Azough, GroenLinks).

[217] Ibid., 2008 (lid Van Beek, VVD). In totaal ging het om zo'n 23 nadere regelingen, voornamelijk AMvRB's.

[218] Ibid., 2009 (lid Brinkman, PVV; cursivering VB). Tevens werd door de PVV de suggestie gedaan om het dragen van een hoofddoek op de paspoortfoto te verbieden; zie ibid., 2010.

[219] Ibid., 2010 (lid Van Beek, VVD).

[220] Ibid., 2010. Zie voor de betreffende wetsgeschiedenis paragraaf 1.1.2 *supra*.

[221] Ibid., 2011.

[222] Ibid.

[223] Ibid., 2016.

[224] Ibid.

[225] Zie de brief van staatssecretaris van Binnenlandse Zaken (Ank Bijleveld-Schouten) d.d. 18 november 2008, *Kamerstukken II*, 2008-2009, 31324, nr. 9.

[226] Ibid., p. 7 (cursivering VB). Zie tevens ibid., p. 1.

[227] Ibid., pp. 2-3 (nadruk en cursivering origineel).

[228] Brief (met bijlage) van staatssecretaris van Binnenlandse Zaken (Ank Bijleveld-Schouten) d.d. 2 december 2008, *Kamerstukken II*, 2008-2009, 31324, nr. 10.

[229] Brief van staatssecretaris Bijleveld d.d. 18 november 2008, *supra* noot 225, p. 6.

[230] Ibid.

[231] Zie *S. and Marper v. United Kingdom*, EHRM 4 december 2008, appl. nos. 30562/04 & 30566/04; *NJCM-Bulletin* 2009, pp. 391-406 (m.nt. M.G.J.M. van der Staak); *EHRC* 2009/13, pp. 148-165 (m.nt. E.J. Koops). Een Nederlandstalige samenvatting van de uitspraak is beschikbaar op www.njcm.nl/site/jurisprudentie/show/51.

[232] Brief van staatssecretaris van Binnenlandse Zaken (Ank Bijleveld-Schouten) d.d. 24 december 2008, *Kamerstukken II*, 2008-2009, 31324, nr. 12, pp. 1-2 (cursivering VB).

[233] Zie behandeling herinrichten reisdocumentenadministratie, *Handelingen II*, 2008-2009, TK 42, 3731-3736 (15 januari 2009).

[234] Ibid., 3734, 3744 (lid Van Raak, SP).

[235] Ibid., 3736-3737 (lid Pechtold, D66).

[236] Ibid., 3738 (lid Azough, GroenLinks).

[237] Ibid., 3744.

[238] Ibid., 3745.

[239] Zie ibid.

[240] Zie ibid., 3746.

[241] Ibid., 3748.

242 Zie Stemmingen, *Handelingen II*, 2008-2009, TK 43, 3768-3769 (20 januari 2009).

243 Zie ibid.

* Bron van figuur: PrivacyBarometer - www.privacybarometer.nl/regels.php?r=19 (met toestemming overgenomen).

244 Zie voorstel van rijkswet tot wijziging van de Paspoortwet in verband met het herinrichten van de reisdocumentenadministratie (20 januari 2009), *Kamerstukken I*, 2008-2009, 31324, A.

245 Zie voorlopig verslag van de vaste commissie voor Binnenlandse Zaken d.d. 24 maart 2009, *Kamerstukken I*, 2008-2009, 31324, B.

246 Zie ibid., pp. 2-3.

247 Zie ibid., p. 3.

248 Zie ibid., p. 2.

249 Zie ibid., pp. 2, 5.

250 Zie ibid.

251 Zie ibid.

252 Zie ibid.

253 Ibid., p. 4.

254 Ibid.

255 Zie ibid.

256 Zie ibid.

257 Zie ibid.

258 Zie memorie van antwoord van de staatssecretaris van Binnenlandse Zaken (Ank Bijleveld-Schouten) d.d. 28 april 2009, *Kamerstukken I*, 2008-2009, 31324, C.

259 Ibid., p. 2.

260 Ibid., p. 3.

261 Zie ibid., pp. 3-4.

262 Ibid., p. 5 (cursivering VB).

263 Zie Portuguese Ministry of the Interior, Internal Security Coordinating Office, *European Identity Systems - a comparative study* (Lisbon, 7 March 2009), p. 25 (figuur met toestemming overgenomen); beschikbaar op www.idfraudconference-pt2007.org/home.php?lg=uk&area=003&mid=004. ISO-codes: AT: Oostenrijk, BE: België, CZ: Tsjechië, DE: Duitsland, ES: Spanje, ET: Estland, FI: Finland, HU: Hongarije, IS: IJsland, LU: Luxemburg, NL: Nederland, PT: Portugal, SI: Slovenië, SK: Slowakije, SW: Zwitserland, UK: Verenigd Koninkrijk. Zie met betrekking tot vingerafdrukken tevens tabel 3.10.2 op p. 24 van het rapport.

264 Bron: email van Fons Knopjes (*managing director* van het ID Management Centre) aan de auteur d.d. 10 augustus 2010.

265 Memorie van antwoord van staatssecretaris Bijleveld d.d. 28 april 2009, *supra* noot 258, pp. 6-7.

266 Ibid., p. 7.

267 Ibid., p. 8.

268 Ibid., p. 9 (cursivering VB).

269 Zie ibid.

270 Ibid., p. 10.

271 Ibid.

272 Zie eindverslag van de vaste commissie voor Binnenlandse Zaken d.d. 12 mei 2009, *Kamerstukken I*, 2008-2009, 31324, D.

273 *Centrale biometrische databank: vloek of zegen*, open brief aan de Eerste Kamer van Annemarie Sprokkereef, Ronald Leenes, Bart Jacobs, Raymond Veldhuis en Max Snijder d.d. 8 juni 2009; beschikbaar op http://vortex.uvt.nl/TILTblog/?p=69#more-69.

274 Behandeling herinrichten reisdocumentenadministratie, *Handelingen I*, 2008-2009, EK 34, 1563 (9 juni 2009).

275 Ibid., 1563-1564 (lid Vliegenthart, SP).

276 Ibid., 1564 (lid Vliegenthart, SP).

277 Ibid., 1565 (lid Vliegenthart, SP).

278 Zie ibid., 1565-1566.

279 Ibid., 1567 (lid Engels, D66).

280 Zie ibid., 1568. Zie in dit verband tevens de vroegere Kamervragen van de leden Vos (GroenLinks), Albayrak (PvdA) en Van der Laan (D66) aan de minister voor Vreemdelingenzaken en Integratie (Rita Verdonk, VVD) over de mogelijke koppeling tussen de besluitvorming rondom biometrie en co-decisie van het Europees Parlement (ingezonden 10 december 2004), *Aanhangsel Handelingen II*, 2004-2005, nr. 754.

281 Behandeling herinrichten reisdocumentenadministratie *supra* noot 274, 1568 (lid Strik, GroenLinks).

282 Zie ibid., 1568-1569.

283 Ibid., 1569 (lid De Vries, PvdA).

284 Ibid., 1570-1571 (lid De Vries, PvdA).

285 Ibid., 1571 (lid De Vries-Leggedoor, CDA). Vergelijk Advies CBP 2007, *supra* noot 184, pp. 6-7.

286 Behandeling herinrichten reisdocumentenadministratie *supra* noot 274, 1571 (lid De Vries-Leggedoor, CDA).

287 Ibid., 1572 (cursivering VB). Vergelijk de relevante wetsgeschiedenis in paragraaf 1.1.2 *supra*.

288 Ibid., 1572 (citaatcorrectie en cursivering VB).

289 Ibid (cursivering VB). Vergelijk de informatie op pp. 75-76 *supra*.

290 Ibid., 1573.

291 Ibid.

292 Zie ibid., 1575-1576.

293 Ibid., 1576. CBP-voorzitter Jacob Kohnstamm zou zich later nogmaals in negatieve zin over de nieuwe Paspoortwet uitlaten; zie *supra*, noot 212.

294 Zie ibid., 1579.

295 Ibid.

296 Ibid.

297 Zie ibid., 1581-1582.

298 Ibid., 1583 (lid Engels, D66).

299 Ibid. (lid Strik, GroenLinks). Zie ook het verslag van een mondeling overleg met minister van Justitie Hirsch Ballin (CDA) d.d. 12 mei 2009, *Kamerstukken I*, 2008-2009, 31386, F, pp. 2-4.

300 Behandeling herinrichten reisdocumentenadministratie *supra* noot 274, 1584.

301 Ibid., 1586.

302 Ibid (cursivering VB).

303 Ibid., 1586-1587.

304 Behandeling hamerstukken, *Handelingen I*, 2008-2009, EK 35, 1593-1594 (16 juni 2009) (cursivering VB).

305 Brief van staatssecretaris Bijleveld (Binnenlandse Zaken) d.d. 17 september 2009, *Kamerstukken II*, 2009-2010, 31324, nr. 23, p. 2 (cursivering VB).

306 Nieuwsbericht agentschap BPR d.d. 21 september 2009 (eerste cursivering VB, tweede origineel).

307 Brief van staatssecretaris Bijleveld (Binnenlandse Zaken) d.d. 19 augustus 2008, *Kamerstukken II*, 2007-2008, 25764, nr. 40, p. 4.

308 MvT bij het wetsvoorstel ter wijziging van de Paspoortwet in verband met het herinrichten van de reisdocumentenadministratie, *supra* noot 173, p. 29. Vergelijk ook ibid., pp. 26-27.

309 Folder *Nieuw reisdocument nodig?*, ministerie van Binnenlandse Zaken, september 2009; beschikbaar op www.rijksoverheid.nl/documenten-en-publicaties/publicaties-pb51/nieuw-reisdocument-nodig.html.

310 Ibid. Zie over het misleidende karakter van deze folder bijvoorbeeld ook Annemarie Sprokkereef, *Vingerafdrukken en het Nederlandse paspoort. Verschuilen achter Brussel?*, Checks&Balances 2010, nr. 1, p. 29; beschikbaar op http://arno.uvt.nl/show.cgi?fid=99566.

311 Ministerie van Binnenlandse Zaken, Paspoortinformatie.nl, onderdeel 'vragen & antwoorden' (versie 4 september 2009, laatstelijk geraadpleegd op 22 augustus 2010): *Waar kan ik bezwaar indienen tegen de opslag van mijn vingerafdrukken in de reisdocumentenadministratie?*; beschikbaar op www.paspoortinformatie.nl/nederlands/Vragen/Vingerafdrukken/Opslag#faq-1.

312 Brief van staatssecretaris Bijleveld (Binnenlandse Zaken) d.d. 17 maart 2010, *Kamerstukken II*, 2009-2010, 25764, nr. 42, p. 3.

313 Ibid., p. 4.

314 Zie *Uw vingerafdrukken bij de Franse militaire industrie*, NRC Handelsblad, 17 maart 2010; *Dit is de dag*, Radio 1, 22 maart 2010.

315 Zie de vragen van het lid Van Raak (SP) over de centrale opslag van vingerafdrukken en over problemen met het opnemen van de vingerafdruk in het paspoort (ingezonden op respectievelijk 16 en 26 maart 2010), *Aanhangsels Handelingen II*, 2009-2010, nrs. 2067 & 2199 (inclusief antwoorden); vragen van het lid Teeven

(VVD) over het NRC-artikel "Uw vingerafdrukken bij de Franse militaire industrie" (ingezonden 19 maart 2010), *Aanhangsels Handelingen II*, 2009-2010, nr. 2280 (inclusief antwoorden).

316 Vragen van het lid Van Raak (SP) *supra* noot 315, nr. 2199, p. 2.

317 Zie Max Snijder, *WRR Case Studie: Black Box Biometrisch Paspoort* (nog te verschijnen).

318 D66, *Anders? Ja, D66!* (april 2010), p. 74.

319 GroenLinks, *Klaar voor de toekomst* (april 2010), p. 40.

320 Partij voor de Dieren, *Recepten voor mededogen en duurzaamheid* (april 2010), pp. 54-55.

321 SP, *Een beter Nederland voor minder geld* (april 2010), p. 24.

322 WRR-interview Grijpink, *supra* tabel 1.1, pp. 2-3.

323 Ibid., p. 4.

324 WRR-interview Van Munster, *supra* tabel 1.1, p. 3.

325 WRR-interview Van Troost, *supra* tabel 1.1, p. 5.

326 Ibid.

327 WRR-interview Van Munster, *supra* tabel 1.1, p. 3.

328 WRR-interview Ruifrok, *supra* tabel 1.1, p. 2. Zie in vergelijkbare zin (maar geredeneerd vanuit betere dienstverlening en lastenverlichting voor de burger) ook WRR-interview Van Troost, *supra* tabel 1.1, p. 5.

329 WRR-interview Grijpink, *supra* tabel 1.1, p. 3. Reeds in juli 2004 (en eerder) had Grijpink zich negatief opgesteld tegenover het biometrische paspoort en gesteld dat identiteits- en *look-alike* fraude hierdoor eerder zouden toe- dan afnemen; zie het artikel van Peter Mom in Automatisering Gids *supra* noot 98, p. 11. Ook in 2001 was Grijpink al relatief kritisch; zie Peter Mom, *Paspoortbiometrie nog ver weg*, Computable, 21 december 2001, p. 7.

330 Jan Grijpink, *Zinvol, betrouwbaar en veilig gebruik van biometrie*, P&I december 2009 (afl. 6), p. 274; beschikbaar op www.biometrieforum.nl/tiki-list_file_gallery.php?galleryId=10.

331 Ibid.

332 WRR-interview Delwel & Koedam, *supra* tabel 1.1, pp. 2-3. Zie ook de vergelijkbare (vroegere) opmerkingen van minister van Justitie Korthals d.d. 10 december 2001, *supra* paragraaf 1.3.

333 WRR-interview Knopjes, *supra* tabel 1.1, p. 6.

334 Zie ibid., pp. 2-3; WRR-interview Grijpink, *supra* tabel 1.1, pp. 3-5.

335 WRR-interview Grijpink, *supra* tabel 1.1, p. 3.

336 WRR-interview Knopjes, *supra* tabel 1.1, p. 3.

337 Zie ibid., p. 3.

338 Zie ibid.

339 Zie ibid., p. 4.

340 Ibid.

341 WRR-interview Grijpink, *supra* tabel 1.1, p. 2.

342 Ibid., pp. 3-5. Overigens had Grijpink zich reeds in november 2004 (in het algemeen) al negatief opgesteld tegenover centrale opslag; zie het interview van Robbert Hoeffnagel met Jan Grijpink in Business Process Magazine 2004, nr. 7, pp. 27-28. Zie voor eenzelfde standpunt van Grijpink van recenter datum bijvoorbeeld *Privacylessen voor technici*, NRC Handelsblad, 1 mei 2010, Wetenschap, p. 8.

343 WRR-interview Grijpink, *supra* tabel 1.1, p. 3.

344 Ibid., p. 4.

345 WRR-interview Provily & Van der Zanden, *supra* tabel 1.1, p. 8. In het Verenigd Koninkrijk was zelfs sprake van afschaffing van biometrische ID-kaarten (en wellicht ook van biometrische paspoorten) en de bijbehorende nationale database; zie hoofdstuk 3 van het Britse regeerakkoord van mei 2010, beschikbaar op www.cabinetoffice.gov.uk/media/409088/pfg_coalition.pdf ("We will implement a full programme of measures to reverse the substantial erosion of civil liberties and roll back state intrusion. (...) We will scrap the ID card scheme, the National Identity register (...) and halt the next generation of biometric passports.") Zie in dit verband vervolgens de *second reading* van de Britse *Identity Documents Bill* d.d. 9 juni 2010, beschikbaar op www.parliament.uk/business/news/2010/06/second-reading-of-identity-documents-bill. Zie ook *Verenigd Koninkrijk trekt stekker uit omstreden identiteitsregister*, Tweakers.net, 28 mei 2010, http://tweakers.net/nieuws/67572/verenigd-koninkrijk-trekt-stekker-uit-omstreden-identiteitsregister.html.

346 WRR-interview Van Munster, *supra* tabel 1.1, p. 4.

347 WRR-interview Van Troost, *supra* tabel 1.1, p. 3.

348 WRR-interview Provily & Van der Zanden, *supra* tabel 1.1, pp. 4-5.

349 Ibid., pp. 2-3.

[350] WRR-interview Knopjes, *supra* tabel 1.1, p. 2. Zie ook WRR-interview Kooij & Levering, *supra* tabel 1.1, p. 2: "Ondanks de invoering van de MRZ [in het paspoort] blijken de voordelen daarvan [op Schiphol] nog niet te worden benut vanwege een gebrek aan controle-infrastructuur (...)."

[351] WRR-interview Van Troost, *supra* tabel 1.1, p. 3.

[352] Zie WRR-interview Van Munster, *supra* tabel 1.1, p. 3.

[353] Ibid.

[354] Ibid., p. 4.

[355] Zie ibid.

[356] Ibid.

[357] WRR-interview Grijpink, *supra* tabel 1.1, pp. 1-2. Zie ook Grijpink in *Privacylessen voor technici*, *supra* noot 342.

[358] NVVB, *Nadere inhoudelijke reactie voorstellen aanpassing Paspoortwet* (B2007/0048, 22 februari 2007, gericht aan agentschap BPR), p. 3.

[359] WRR-interview Grijpink, *supra* tabel 1.1, p. 2.

[360] Online Raadpleegbare Reisdocumenten Administratie. ('ORRA' is de ambtelijke jargonterm voor de (nog te ontwikkelen) centrale reisdocumentenadministratie.)

[361] WRR-interview Knopjes, *supra* tabel 1.1, p. 5.

[362] Ibid., pp. 6-7.

[363] WRR-interview Ruifrok, *supra* tabel 1.1, p. 4. Zie reeds jaren eerder (2004) in vergelijkbare zin Jan Grijpink in Automatisering Gids, *supra* noot 98, p. 11: "Vóór zijn daad is een terrorist een gewone, nette burger. Biometrie zal onbekende daders niet tegenhouden."

[364] WRR-interview Van Munster, *supra* tabel 1.1, p. 4.

[365] Zie WRR-interview Ruifrok, *supra* tabel 1.1, p. 2.

DEEL B *VOICES FROM GROUND CONTROL*: DE AANNAME VAN DE NIEUWE PASPOORTWET ALS MAATSCHAPPELIJK *TRIGGER EVENT*

"How can I help seeing what is in front of my eyes? Two and two are four."
"Sometimes, Winston. Sometimes they are five. Sometimes they are three.
Sometimes they are all of them at once. You must try harder. It is not easy to become sane."[*]

---

* George Orwell, *Nineteen Eighty-Four*, p. 201 (editie Penguin 1976).

3 DE STILTE ROND HET BIOMETRISCHE PASPOORT DOORBROKEN

Tijdens de parlementaire behandeling van de nieuwe Paspoortwet had er vrijwel geen (hoorbare) maatschappelijke kritiek op geklonken. De meest waarschijnlijke verklaring voor deze 'thundering silence' is tweeledig: 1) het wetsvoorstel was beide Kamers relatief vlot en geruisloos gepasseerd, en 2) in de reguliere media (met name ook op televisie[1]) werd er nauwelijks aandacht aan besteed. Op NRC Handelsblad[2] en de Volkskrant[3] na kwam daadwerkelijke media-aandacht pas op gang nadat het wetsvoorstel reeds enkele weken was aangenomen: eind juni 2009 was er een eerste golf van kritische berichtgeving over de nieuwe Paspoortwet.[4] Mensenrechtenorganisaties roerden zich en nieuwe belangengroeperingen schoten als paddenstoelen uit de grond.[5] Een korte beschrijving van deze ontwikkelingen volgt hieronder, te beginnen met de eerste organisatie die haar kans schoon zag om een en ander direct op het allerhoogste niveau aan te kaarten: het Nederlands Juristen Comité voor de Mensenrechten.

3.1 Het biometrische paspoort op de agenda van het VN-Mensenrechten-comité

Amper twee weken nadat de nieuwe Paspoortwet door de Eerste Kamer was aangenomen, werd de hieruit voortvloeiende centrale reisdocumentenadministratie door een brede coalitie van Nederlandse NGO's op de agenda gezet van het Mensenrechtencomité van de Verenigde Naties in Genève. Het initiatief hiertoe kwam van het Nederlands Juristen Comité voor de Mensenrechten (NJCM)[6] en werd gesteund door Aim for Human Rights (voormalig Humanistisch Overleg Mensenrechten), Artikel 1, de CG-Raad, COC Nederland, de Johannes Wier Stichting, Justitia et Pax, het Netwerk VN-Vrouwenverdrag en VluchtelingenWerk Nederland. Het VN-Mensenrechtencomité beoordeelt periodiek[7] de Nederlandse naleving van het Internationale Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR). Dit gebeurde voor het laatst in juli 2001.[8] De eerstvolgende sessie waarin Nederland door dit Comité zou worden beoordeeld zou in Genève plaatsvinden op 14 en 15 juli 2009. Onder het relevante agenda-item 'counterterrorism measures and respect for rights guaranteed in the Covenant'[9] werd een en ander op 25 juni 2009 door de Nederlandse NGO-coalitie onder leiding van het NJCM als volgt aangekaart:

> "*National fingerprint database*
> In order to implement the European regulation on passport security, the Netherlands has recently passed a law which introduces biometric passports containing an RFID-microchip with digital information about the passport owner. Under the European regulation, a digital facial image and the fingerprints of the passport owner will have to be stored on this microchip for identification purposes and in order to prevent fraudulent use. However, by storing the data of all biometric passports in a central database for criminal investigation purposes (including counter-terrorism), the Netherlands has gone one giant leap further than the European

> regulation. This 'national fingerprint database' will thus come to include the fingerprints of every Dutch citizen, regardless of any criminal activity, hence turning people's travel documents for personal use into security documents for use by the State. Citizens will hardly have any control over the biometric information stored about them. Many experts have also warned that data breaches and identity theft are inevitable. Both the Dutch Data Protection Authority and other experts have consequently found this new law on biometric passports to be in serious violation of the right to privacy. The Dutch NGOs accordingly urge the Human Rights Committee to address this grave breach of Article 17 ICCPR in its upcoming session."[10]

De 26-koppige Nederlandse delegatie voor de sessie werd geleid door minister van Justitie Hirsch Ballin (CDA). Het Britse lid van het VN-Mensenrechtencomité (Sir Nigel Rodley) stelde het punt van de centrale opslag van vingerafdrukken tijdens de eerste sessiedag nadrukkelijk aan de orde en merkte daarbij onder andere het volgende op: "Het schijnt namelijk erg makkelijk te zijn om zulke data kwijt te raken. Daar weet mijn land alles van."[11] (In het Verenigd Koninkrijk waren in 2007 twee cd's van de belastingdienst met gegevens van 25 miljoen Britten zoekgeraakt.) Over de opslag van biometrische gegevens benadrukte Sir Rodley tevens dat mensenrechten niet een willekeurig afwegingsproces vormen. "De criteria moeten telkens opnieuw zeer zorgvuldig worden onderzocht."[12] De VN-notulen van de sessie vermelden over de vragen van Rodley en de antwoorden van minister Hirsch Ballin verder het volgende:

> "Clarifications would (...) be welcome on the new legislation providing for the inclusion of biometric data in Netherlands travel documents. Some non-governmental organizations claimed that a national database would be established using that information. Would the information be included in the passport, was it already used in identity cards, to what end was it used, what would happen to the data afterwards and what access would the persons concerned have to it? In any event, the State party must ensure that the right to privacy was safeguarded."[13]
>
> "In reply to the question about biometric passports, [Mr. Hirsch Ballin] said that it was common practice to store information on passports and other travel information in databases. The central storage of that data provided the best guarantee of adequate protection. The high standards of protection in the Netherlands did not permit even the Public Prosecutor to access that data without specific reasons, which were enumerated in the relevant legislation."[14]

Daarnaast was er na afloop van de eerste sessiedag echter nog een opmerking van minister Hirsch Ballin die in Nederland enige beroering wekte.[15] Tegenover twee Nederlandse journalisten had de minister in Genève gezegd dat het niet uitgesloten was dat de vingerafdrukken in het paspoort "op termijn" zouden worden vervangen door irisscans.[16] Diezelfde avond verklaarde de minister tegenover BNR Nieuwsradio verder nog het volgende: "Uit een oogpunt van bescherming van privacy, van rechten van de mens, is het goed dat er een centrale opslag is, want [*sic*] dat moet ook héél goed worden beveiligd. Niet toegankelijk voor nieuwsgierige blikken, ook niet zomaar voor overheidsinstanties. Zelfs het Openbaar Ministerie kan alleen toegang krijgen tot die gegevens als er een bijzondere reden voor is; een verdenking die op iemand betrekking heeft."[17]

In de *Concluding Observations* van het Mensenrechtencomité (eind juli 2009) kwam het punt van de centrale opslag van vingerafdrukken niet specifiek terug. Desgevraagd liet Sir Rodley de oorzaak hiervan in het midden en gaf slechts in het algemeen aan dat "[r]easons could range from accidental oversight to lack of agreement (which may be deep or merely a matter of uncertainty that there isn't enough time to talk through) about the existence or nature of a problem under the Covenant."[18] Het onderwerp in kwestie zou echter wel kunnen worden 'ingelezen' in de volgende algemene aanbeveling van het Comité:

> "The [Netherlands] should amend its legislation to ensure that its counter-terrorism measures do not conflict with article 17 of the Covenant and that effective safeguards, including judicial oversight, are in place to counter abuses."[19]

In de parlementaire Kabinetsreactie naar aanleiding van de *Concluding Observations* werd niet aan de vragen van het Mensenrechtencomité over de nieuwe Paspoortwet gerefereerd.[20] Tot Kamervragen of -moties heeft de VN-sessie (die behalve over privacy ook over talrijke andere Nederlandse mensenrechtenkwesties ging) tot nu toe evenmin geleid.

3.2 Poging tot schorsing van inwerkingtreding van de nieuwe Paspoortwet bij het Europese Hof voor de Rechten van de Mens

Enkele dagen nadat het VN-Mensenrechtencomité zijn *Concluding Observations* had uitgevaardigd, werd een volgende internationaal-juridische poging om de inwerkingtreding van de nieuwe Paspoortwet tegen te houden ondernomen door de vereniging Vrijbit.[21] De inwerkingtreding van de wet stond gepland voor maandag 21 september 2009. Op 2 augustus 2009 verzocht Vrijbit het Europese Hof voor de Rechten van de Mens (EHRM) om Nederland middels een voorlopige maatregel (*Rule 39*-procedure) te verbieden de nieuwe Paspoortwet in te voeren. De kernpassages uit dit spoedverzoek van Vrijbit aan het EHRM luidden als volgt:

> "Namens de leden van de vereniging Vrijbit dienen we bij deze een klacht in tegen de Staat der Nederlanden wegens schending van artikel 8 EVRM betreffende het recht op privéleven. Dit omdat vanaf 21 september digitale pasfoto's en vingerafdrukken in één centraal paspoortregister worden geregistreerd, samen met alle overige persoonsgegevens die vermeld worden op een paspoort of ID-kaart. Data die aan inlichtingen- en veiligheidsdiensten en indirect ook aan Justitie ter beschikking worden gesteld. (...) De registratie van biometrische kenmerken in een centrale database is van meet af aan bekritiseerd door experts in informatiebeveiliging. (...) Naar hun mening wordt de burger definitief de mogelijkheid ontnomen om controle te houden over zijn of haar gegevens. De overheid kijkt niet alleen meer of een paspoort/ID-kaart bij een persoon hoort, maar kan elke burger identificeren aan de hand van een ergens aangetroffen vingerafdruk. Hierdoor wordt feitelijk iedereen als potentiële verdachte of terrorist bestempeld. (...)
>
> Onze klacht betreft:
> 1. De invoering van één centraal paspoortregister met alle gegevens voor uitgifte van paspoorten/IDkaarten.
> 2. Het opslaan van onze biometrische gegevens - foto's en vingerafdrukken - in een centrale paspoortadministratie.
> 3. Het gebruik van biometrische gegevens door inlichtingen- en veiligheidsdiensten.

4. Bevoegdheid van Officier van Justitie om paspoortgegevens, inclusief biometrische gegevens, op te vragen voor justitiële doeleinden.
5. De totstandkoming van de wetswijziging, waarbij over de inperking van de privacy vooraf geen gedegen onderzoek heeft plaatsgehad of deze noodzakelijk is en het doel niet op een andere – minder belastende – wijze te verwezenlijken is, en of voldaan wordt aan het proportionaliteitsbeginsel volgens de bepalingen van artikel 8 EVRM.
6. Het risico dat onze veiligheid individueel in gevaar wordt gebracht door de registratie van onze persoonsgegevens in één centrale database.
7. Het risico dat het gehele bevolkingsregister in handen van onbevoegden of kwaadwillenden komt.
8. Het risico dat onze gegevens in handen komen van mogendheden, waar geen afdoende wet- en regelgeving bestaat ter bescherming van persoonsgegevens.

(...)
Wij zijn ons zeer wel bewust dat een klacht bij het Europese Hof officieel pas kan worden ingediend nadat op nationaal niveau alle juridische mogelijkheden zijn beproefd en uitgeput. Er bestaat in Nederland echter geen rechtsmiddel dat kan voorkomen dat op 21 september aanstaande de centrale biometrische reisdocumentenadministratie wordt opgestart en daarmee de aantasting van onze persoonlijke levenssfeer een feit wordt. Dit komt omdat het paspoort en de ID-kaart in Nederland niet slechts reisdocumenten zijn, maar voor Nederlandse burgers ook voor binnenlands gebruik een geldig paspoort/IDkaart een vereiste is. Wie niet over zo'n geldig document beschikt is uitgesloten van het maatschappelijk verkeer aangezien men geen arbeidscontract mag afsluiten, geen uitkering kan ontvangen, geen huis kan kopen, geen (verplichte) zorgverzekering kan afsluiten, zich niet kan inschrijven bij een onderwijsinstelling en zelfs het risico loopt om gearresteerd te worden zonder dat men zich schuldig maakt aan enig strafbaar feit. Hierdoor staan wij op nationaal niveau praktisch machteloos om de immense inperking van onze burgerrechten aan te vechten.
(...)
Pas als op 21 september mensen daadwerkelijk weigeren om – onder de huidige condities – hun vingerafdrukken te laten afnemen om een geldig paspoort/IDkaart te krijgen, ontstaat de situatie dat de overheid weigert om hen een geldig identiteitsbewijs te verstrekken. Niet nadat de betrokken persoon daarvan een officiële beschikking heeft verkregen kan er bezwaar worden aangetekend (...). Dan is het a) te laat om de opstart van de centrale database tegen te houden, en kan b) de politie iemand niet alleen arresteren wegens het niet kunnen tonen van een geldig identiteitsbewijs, maar heeft men ook de bevoegdheid om foto's en vingerafdrukken van de betrokken persoon op te slaan in een strafketendossier. Zo zitten wij, als onschuldige burgers, in de tang: enerzijds hebben we geen juridische mogelijkheid om tijdig de invoering tegen te houden van een paspoortregistratiesysteem waarbij onze gegevens voor opsporingsdoeleinden beschikbaar komen, en anderzijds lopen we het gevaar dat onze biometrische gegevens rechtreeks in justitieregisters worden opgeslagen als we niet toestaan dat onze gegevens in een dergelijke paspoortdatabank worden geregistreerd.

Vandaar dat wij u bij deze vragen om, bij voorlopige maatregel, de opname van biometrische gegevens zoals digitale foto's en vingerafdrukken in één centrale paspoortdatabase door de Nederlandse overheid stop te zetten. (...)"[22]

NRC Handelsblad schreef over het verzoek van Vrijbit:

"Aan deze procedure kleven juridische haken en ogen. Voordat een gedupeerde mag klagen bij het EHRM, moeten alle nationale rechtsmiddelen zijn uitgeput. Dat is hier niet het geval. De wet is nog niet in werking getreden, laat staan dat er al procedures over gevoerd zijn. Michiel van Emmerik, hoofddocent staats- en bestuursrecht aan de Universiteit Leiden: 'Alleen bij hoge uitzondering wordt hiervan afgeweken. Bijvoorbeeld als een procedure evident geen kans van slagen heeft'.

Verder is het de vraag of Vrijbit als vereniging klachtrecht heeft. Op zichzelf kunnen niet-gouvernementele organisaties procederen bij het EHRM. Van Emmerik: 'Maar er moet dan wel iemand individueel geraakt zijn.' En het EHRM neemt alleen in uitzonderlijke gevallen spoedmaatregelen aan, bijvoorbeeld als een klager dreigt te worden uitgezet naar een land waar hem de doodstraf wacht.

> [Vrijbit-voorzitter Miek] Wijnberg is zich van deze obstakels bewust. ‘Onze leden *zijn* al gedupeerd. Zij maken zich druk over het feit dat zij gedwongen worden zo’n document te nemen. Zo niet, word je uit de maatschappij gezet’. Wijnberg doelt er op dat een paspoort niet alleen een reisdocument is. ‘Zonder paspoort of identiteitskaart kun je geen arbeidscontract sluiten, geen uitkering aanvragen en geen huis kopen’.”[23]

Op 24 augustus 2009 werd het spoedverzoek van Vrijbit door het EHRM middels een standaardformule afgewezen:

> “I acknowledge receipt (...) of your letter (...) requesting the European Court of Human Rights to indicate to the Government of the Netherlands, by way of interim measure (*voorlopige maatregel*), to halt the storage of biometric data in a central passport database. (...) In the present case, the situation you have outlined in your letter is not one of those in which the measure provided for in Rule 39 [of the Rules of Court] can be applied. Interim measures are indicated only in limited spheres. (...) [I]n practice the Court only applies Rule 39 if there is an imminent risk of irreparable damage. While there is no specific provision in the Convention concerning the domains in which Rule 39 will apply, requests for its application usually concern the right to life (Article 2), the right not to be subjected to torture or inhuman treatment (Article 3) and, exceptionally, the right to respect for private and family life (Article 8) or other rights guaranteed by the Convention. The vast majority of cases in which interim measures have been indicated concern deportation and extradition proceedings (...).”[24]

Hierop diende Vrijbit nogmaals eenzelfde, nader onderbouwd verzoek in bij het EHRM.[25] “Opslag [vinger]afdrukken onzeker”, kopte nu ook de Volkskrant en berichtte als volgt:

> “De opslag van vingerafdrukken in een centraal databestand is niet zeker. Het Europese Hof voor de Rechten van de Mens heeft bekendgemaakt vrijdag uitspraak te doen over deze operatie. (...) De vereniging Vrijbit legde zich er niet bij neer. Die vroeg een voorlopige voorziening aan het Europese Hof, in afwachting van een bodemprocedure bij hetzelfde Hof. Tot nu toe was niet zeker of die voorlopige voorziening er voor maandag [21 september] zou zijn, maar gisteren meldde het Hof vrijdag met een uitspraak te komen. Binnenlandse Zaken wil niet ingaan op de vraag wat er gaat gebeuren als het Hof de opslag van de vingerafdrukken verbiedt.”[26]

Op vrijdag 18 september 2009 werd het herziene spoedverzoek van Vrijbit wederom door het EHRM afgewezen, opnieuw zonder inhoudelijk op de zaak in te gaan.[27] Een persbericht van Vrijbit lichtte een en ander als volgt toe:

> “Het Europese Hof voor de Rechten van de Mens heeft op 18 september aan Vrijbit bevestigd dat er geen interim-maatregelen kunnen worden genomen tegen de registratie en opslag van vingerafdrukken van Nederlanders vanaf 21 september. Vrijbit had deze week haar eerdere verzoek om schorsing van de registratie en opslag van biometrische gegevens herhaald en verder juridisch onderbouwd. Het Hof in Straatburg legde dit, zonder hier inhoudelijk op in te gaan, opnieuw terzijde.
>
> Interim-maatregelen door het Hof worden alleen getroffen als er onherstelbare schade dreigt door een vermeende mensenrechtenschending. Bijvoorbeeld als een vluchteling dreigt te worden uitgezet naar een land waar zijn leven in gevaar komt, kan het Hof ingrijpen. Naar analogie hiervan had Vrijbit aangevoerd dat door de privacyschendende opslag van foto en vingerafdrukken de ‘digitale persoonlijkheid’ van de Nederlander in levensgevaar komt als deze vanaf 21 september wordt uitgeleverd aan de onveilige wereld van de databanken. Onherstelbare schade dreigt in dat geval. Algemeen bekend is dat vooral het terughalen en achteraf verwijderen van biometrische gegevens uit de verschillende datasystemen en -bestanden, in binnen- en buitenland, in de praktijk een illusie is. Technisch is dit herstel niet voor honderd procent te garanderen en zijn foutmarges onvermijdelijk. Wet- en regelgeving zijn er bovendien niet op toegerust om te bepalen onder wiens bevoegdheid en

verantwoordelijkheid dit terughalen en verwijderen zou dienen te gebeuren. En als gegevens in handen vallen van onbevoegden, is het glashelder dat de Nederlandse regering aan slachtoffers geen garantie kan geven dat zij de (inmiddels gekoppelde, doorgegeven of doorverkochte) gegevens nog verwijderd kunnen krijgen.

Daarom eiste Vrijbit een schorsing van de opslag van biometrische gegevens in het paspoort en de Identiteitskaart, totdat de bodemprocedure hiertegen is afgesloten. Het Hof is niet inhoudelijk op deze argumentatie ingegaan, maar verklaarde, zonder opgaaf van redenen, het schorsingsverzoek van Vrijbit niet-ontvankelijk. Desondanks ziet Vrijbit de bij het Hof aangespannen bodemprocedure tegen de Paspoortwet met vertrouwen tegemoet."[28]

Tijdens de plenaire ochtendsessie van een congres van het NJCM in oktober 2009 verklaarde de Nationale ombudsman (Alex Brenninkmeijer) tegenover een lid van Vrijbit publiekelijk "de basis van de uitspraak [van het EHRM] niet zo heel erg degelijk" te vinden, aangezien de centrale opslag van biometrische gegevens "natuurlijk wel een onomkeerbaar gevolg" had.[29] Een andere belangwekkende opmerking in dit verband werd tijdens hetzelfde congres gemaakt door de Europees Toezichthouder voor Gegevensbescherming (Peter Hustinx, tevens voormalig voorzitter van het CBP):

"Nederland is het enige land in Europa dat niet alleen biometrische kenmerken in het paspoort heeft staan, maar ook de gelegenheid heeft aangegrepen om één centrale database van biometrische kenmerken op te gaan bouwen. Dat is het perspectief. Nou moet ik hier gezegd hebben dat de invoering in 2004 van biometrie als een vereiste, wat mij betreft, wat te vroeg is gekomen. Want, zo supersolide is het allemaal nog niet. En biometrie is naar zijn aard gebaseerd op waarschijnlijkheid, en er is dus ook een kans, en die ligt soms in de orde van 1-2%, dat het niet dezelfde persoon is. En daarom moet je daar heel zorgvuldig mee omgaan en allerlei strategieën daaromheen ontwikkelen. Dat is één probleem. Maar, wanneer je een kenmerk dat bedoeld is om identiteitsfraude tegen te gaan, en het ultieme wapen, opslaat in een centrale database in een omgeving waarin de overheid wellicht structureel de kwaliteitseisen onderschat, dan kun je, vrees ik, de klok gelijk zetten op een rampzalige gebeurtenis. En ik denk dus dat de staatssecretaris van Binnenlandse Zaken, die in de Eerste Kamer met dat vraagstuk is geconfronteerd door de oppositie en toen als enige antwoord gaf: 'Als dat probleem zich voordoet, dan lossen we het op', het misschien toch allemaal wat onderschat."[30]

Sindsdien wacht de door Vrijbit bij het EHRM aangespannen bodemprocedure[31] nog op behandeling.

3.3 Kritische vragen over de Paspoortwet vanuit het Europees Parlement

Enkele dagen nadat de poging van het NJCM om de nieuwe Paspoortwet op VN-niveau aan de mensenrechten te laten toetsen vergeefs was gebleken, werd diezelfde (on)verenigbaarheid ook op Europees politiek niveau aan de kaak gesteld: op 5 augustus 2009 stelde de Nederlandse Europarlementariër Jeanine Hennis-Plasschaert (VVD) hiertoe een aantal kritische vragen aan de Europese Commissie:

"Nederland heeft inmiddels besloten om tot centrale opslag van de biometrische gegevens én een daaraan gekoppelde opsporingsfunctie over te gaan. Hiermee zijn de Nederlandse autoriteiten voorbijgegaan aan scherpe kritiek vanuit binnen- en buitenland en is in feite elke Nederlander op voorhand verdachte. Onder andere function creep, fraude en verkeerd gebruik

(dan wel: misbruik) zijn reële risico's. Verder zijn de recente uitspraken van de Nederlandse minister van Justitie voor het Internationaal Comité voor de Mensenrechten van de VN ('de vingerafdruk zou moeten worden vervangen door een iriscode') op z'n zachtst gezegd opvallend te noemen.

1. Is de Commissie door Nederland geconsulteerd over het voornemen om tot een centrale opslag van de biometrische gegevens én een daaraan gekoppelde opsporingsfunctie over te gaan?
2. Hoe beoordeelt de Commissie de nieuwe Nederlandse paspoortwet in het kader van het proportionaliteitsbeginsel? Graag een concreet antwoord.
3. Hoe beoordeelt de Commissie de nieuwe Nederlandse paspoortwet in het kader van de privacy en persoonlijke levenssfeer? Graag een concreet antwoord.
4. Is de Commissie van mening dat de nieuwe Nederlandse paspoortwet in overeenstemming is met artikel 8 EVRM? Zo ja, waarom? Zo nee, waarom niet?
5. Is de Commissie van mening dat voor een effectieve bestrijding van identiteitsfraude het uitsluitend opnemen van biometrie in paspoort in feite voldoende is? Zo nee, waarom niet?
6. Is de Commissie van mening dat, áls er al besloten wordt tot opslag in database, een decentrale opslag (met centrale verwijsindex) zou volstaan? Zo nee, waarom niet?"[32]

Hierop volgde enkele weken later een ontwijkende reactie van de Commissie; in deze reactie bleven alle gestelde vragen in wezen onbeantwoord. Ook werd in het antwoord van de Commissie in het geheel niet (concreet) ingegaan op de mensenrechtelijke aspecten van de nieuwe Nederlandse Paspoortwet.[33] Hennis-Plasschaert herhaalde hierop haar vragen aan de Commissie en deelde de Commissie tevens mee dat zij "[d]e algemeenheden zoals verwoord in de reactie van 25 augustus jl. (...), met alle respect, onvoldoende serieus [kon] nemen."[34] Vervolgens antwoordde de Commissie als volgt:

"1. De Nederlandse regering heeft, aangezien zij daartoe niet verplicht is, de Commissie *niet geraadpleegd* over haar voorstel om biometrische gegevens centraal op te slaan en daaraan een opsporingsfunctie te koppelen.
2. Daar het opzetten van nationale gegevensbanken krachtens nationaal recht *niet onder het Gemeenschapsrecht* valt, is het niet aan de Commissie om op dit aspect van de nieuwe Nederlandse paspoortwet commentaar te leveren. In het belang van de openbare veiligheid of de bescherming van de openbare orde kan het noodzakelijk zijn de identiteit van een persoon vast te stellen met gebruikmaking van gegevens die in een nationaal gegevensbestand zijn opgeslagen, dus aan de hand van maatregelen die bij nationale wetgeving zijn getroffen om een betrouwbare identificatie van paspoorthouders te garanderen door middel van de verwerking van biometrische gegevens, ten einde het gebruik van fictieve identiteiten en fraude, waaronder ook 'identiteitsdiefstal', te voorkomen en op te sporen. (...)
4. Het opzetten van nationale gegevensbanken en de keuze voor een gecentraliseerde dan wel gedecentraliseerde gegevensopslag *op gebieden die niet onder het Gemeenschapsrecht vallen*, is een zaak van het nationale recht."[35]

Dit noodzaakte Hennis-Plasschaert tot een derde (en zelfs vierde) poging:

"De Commissie geeft (...) aan dat het niet aan de Commissie is om op dit aspect (te weten: centrale database waarin o.a. opgenomen de vingerafdrukken van alle Nederlanders + de daaraan gekoppelde opsporingsfunctie) van de nieuwe Nederlandse paspoortwet commentaar te leveren. Dit wekt op z'n zachtst gezegd enige verbazing. (...)
1. Kan de Commissie derhalve precies aangeven hoe zij haar rol als hoedster van de Verdragen (en dus ook de fundamentele rechten) meent in te vullen? (...)

2. Kan de Commissie verder precies aangeven of (en zo ja, op welke wijze) deze inbreuk op het grondrecht tot eerbiediging van de persoonlijke levenssfeer kan worden gerechtvaardigd? Zo nee, waarom niet?

(...)

5. Een meldplicht voor overheidsinstanties dat hun systeem gekraakt is, bestaat niet. Mechanismen voor transparantie over veiligheid en kwetsbaarheid van systemen zijn er niet. Effectieve rechtsbescherming voor burgers (er zijn immers vele factoren die een foutieve of gemanipuleerde registratie van de biometrische gegevens kunnen opleveren waardoor de centrale database vervuild raakt en aldus onbetrouwbare uitkomsten oplevert) ontbreekt. Is het niet hoog tijd dat de veiligheid en beveiliging van het arsenaal aan technische systemen op een meer systematische en integrale wijze de aandacht van de Commissie krijgt? Zo nee, waarom niet?"[36]

Wederom volgde een ontwijkend antwoord van de Commissie:

> "Iedere burger heeft het recht op grond van het nationale recht bij een nationale rechtbank beroep aan te tekenen tegen een bestuurlijke maatregel. De Commissie mag als 'hoedster van de Verdragen' (...) slechts optreden wanneer een lidstaat zijn verplichtingen op grond van het Verdrag of van besluiten van de Gemeenschap niet is nagekomen. Zij ziet toe op de veiligheid en de beveiliging van de technische systemen voor de databases waarvoor zijzelf verantwoordelijk is, maar *kan geen verantwoordelijkheid nemen voor nationale databases die op grond van het nationale recht tot stand zijn gekomen*."[37]

Het restant van het antwoord van de Commissie bestond grotendeels uit verdere herhalingen en algemeenheden. Het laatste woord in deze reeks van vragen en antwoorden leek dan ook nog niet te zijn gezegd, ware het niet dat Hennis-Plasschaert haar positie als Europarlementariër voortijdig verruilde voor het lidmaatschap van de VVD-fractie in de Tweede Kamer. Tot mildere kritiek op de Paspoortwet leidde dit bij haar echter niet. Integendeel:

> "In feite zijn 16 miljoen Nederlanders hiermee op voorhand verdachte (...). Ik vind het ongelooflijk dat een meerderheid in de Tweede Kamer hiermee akkoord is gegaan. Er wordt wel gezegd dat het geen database is om lekker in rond te shoppen, maar die waarborgen zijn nog niet in de wet vastgelegd. Demissionair staatssecretaris Bijleveld van Binnenlandse Zaken zegt in feite: vertrouw me op mijn blauwe ogen dat we niets verkeerds doen met die gegevens. Nu wil ik daar in het geval van het CDA nog best vanuit gaan, maar straks zit er misschien een andere partij in de regering die daar heel anders over denkt. (...) Al die sprookjesverhalen dat het van Brussel moest komen mijn neus uit. Het biometrisch paspoort is er gekomen om identiteitsfraude te bestrijden. Als je de vingerafdrukken vervolgens ook centraal gaat opslaan en gaat gebruiken voor het bestrijden van criminaliteit laat je dat doel helemaal los."[38]

3.4 Grootschalige folderactie tegen centrale opslag van vingerafdrukken

Op 23 november 2009 werd in een groot aantal Nederlandse steden (waaronder Amsterdam, Utrecht, Rotterdam en Den Haag) een huis-aan-huisfolder verspreid die qua stijl en logo afkomstig leek te zijn van de overheid.[39] In deze folder van 'Het Nieuwe Rijk' werden burgers opgeroepen om gratis hun burgerservicenummer op hun arm te laten tatoeëren. Dit zodat men hiermee "nog eenvoudiger geïdentificeerd" zou kunnen worden.[40] Voor meer informatie werd de lezer doorverwezen naar de gemeente. Al snel bleek Het Nieuwe Rijk een initiatief te zijn van een collectief van "bezorgde burgers" onder de naam *2 Plus 2 Makes 4*.[41] De

satirische folderactie werd gesteund door een aantal bekende Nederlanders en was bedoeld om een “aanzet te geven tot een publiek debat over de aanleg van de centrale database met vingerafdrukken.”[42] Het eerste persbericht van Het Nieuwe Rijk verklaarde de actie als volgt:

> “De actie beoogt de burger te confronteren met de risico’s van de opslag van vingerafdrukken in een centrale database. Het collectief wil een brede discussie aanwakkeren over het nut en de juridische legitimiteit van de database en de toenemende verzameldrift van de Nederlandse overheid in het algemeen. Dat de overheid in een persbericht heeft gewaarschuwd voor de folder onderstreept alleen maar dat deze discussie hard nodig is.
>
> De wet is weliswaar al aangenomen, maar de centrale database moet nog worden aangelegd. Het doel van het collectief is dat zoveel mogelijk mensen zich uitspreken tegen deze database door middel van een online petitie, welke vandaag is gestart op www.hetnieuwerijk.nl. Deze is al ondertekend door diverse sympathisanten, waaronder Bob Fosko, Maarten van Roozendaal en Henk Schiffmacher. Middels de petitie wordt de Nederlandse regering opgeroepen om het besluit tot het aanleggen van de database terug te draaien.”[43]

De actie van Het Nieuwe Rijk kreeg massale aandacht in de media.[44] Ondanks enkele eerste negatieve reacties (waaronder van het CIDI, in verband met vermeende associaties met de Holocaust[45]), een landelijk verspreide overheidswaarschuwing voor de folder[46] en strafrechtelijke aangifte tegen Het Nieuwe Rijk door staatssecretaris Bijleveld (die de folder tevens misleidend en ‘smakeloos’ noemde[47]), waren de meeste commentaren overwegend positief.[48] Volgens de directeur van het Rathenau Instituut had de ‘tatoeagefolder’ zelfs “iets bereikt wat instituten zoals het mijne al jaren met adviezen en rapporten proberen te bewerkstelligen: de overheid doen beseffen dat er echt wat aan de hand is. De overheid ervan doordringen dat welke goede redenen er ook zijn om data te verzamelen, te delen en te aggregeren, de prijs die we ervoor betalen erg hoog is: het eroderen van het vertrouwen tussen burger en staat.”[49]

Het Nieuwe Rijk zelf reageerde als volgt op alle commotie:

> “We hebben begrepen dat staatssecretaris Bijleveld aangifte doet. Naar de mening van Het Nieuwe Rijk is dit volstrekt kansloos, omdat het hier duidelijk een persiflage betreft. Deze reactie laat bovendien zien dat het niet goed gesteld is met de vrijheid van meningsuiting in Nederland. Het feit dat deze folder bestempeld wordt als een uitgave die van de overheid afkomstig kan zijn, bewijst dat het misschien niet zo ver van de werkelijkheid ligt.
>
> We zijn ons er van bewust dat deze actie aan gevoeligheden raakt, maar dit was nodig om een grote publieke discussie te starten. We creëren nu in Nederland dezelfde voorwaarden en middelen waardoor het eerder al eens helemaal mis heeft kunnen gaan. Gezien de geschiedenis hopen wij juist op sympathie van slachtoffers van de Tweede Wereldoorlog. En dat ook zij zich uitspreken tegen de opslag van vingerafdrukken en andere gevoelige persoonlijke informatie. Het aanleggen van dergelijke databases is een vrijwel onomkeerbaar proces en het is onmogelijk om te zeggen wie hier in de toekomst toegang tot zal hebben.
>
> De centrale database is er nog niet, druist in tegen onze grondrechten en het Europees Verdrag voor de Rechten van de Mens. Bovendien maakt het Nederland niet perse veiliger. Wij vragen de Nederlandse bevolking daarom om via de online petitie onze regering op te roepen deze wet terug te draaien.”[50]

Twee dagen later (er was nog steeds volop discussie over de folder) nodigde Het Nieuwe Rijk de staatssecretaris uit om publiekelijk, op televisie, het gesprek met hen aan te gaan over de onderliggende kwestie: de centrale database waarin vingerafdrukken zouden worden opgeslagen.[51] Tot op heden is de (inmiddels demissionaire) staatssecretaris niet op deze uitnodiging ingegaan.

Op 11 januari 2010 liet het Openbaar Ministerie (OM) weten niet tot vervolging van Het Nieuwe Rijk te zullen overgaan:

> "Het OM heeft naar aanleiding van de aangifte onderzocht of er door het maken en verspreiden van deze folder sprake was van een strafbaar feit. Het OM is van mening dat de folder smakeloos is, maar dat er geen sprake is van een strafbaar feit. Veel mensen zullen een associatie hebben met de jodenvervolging in de WOII en het is begrijpelijk dat zeker Joodse mensen zich gekwetst zullen voelen als zij met de folder worden geconfronteerd. Maar daarmee is nog geen sprake van strafbare discriminatie.
>
> Voor de vraag naar de strafbaarheid is doorslaggevend dat er in de folder niets (beledigends) wordt gezegd over Joden in het algemeen en er worden ook geen conclusies getrokken ten aanzien van Joden. Er wordt voorts niet in het openbaar aangezet tot haat of geweld of het discrimineren van mensen wegens hun ras en/of godsdienst. Om die redenen is er geen sprake van strafbare discriminatie.
>
> Daarnaast is er volgens het OM ook geen sprake van een strafbare valsheid of vervalsing (door de folder te laten lijken op de overheidshuisstijl). De folder was namelijk *niet gemaakt met het oogmerk om deze als echt/onvervalst te laten doorgaan*. Dit is o.a. ook te zien aan het onjuist weergeven van het overheidslogo. De folder is *opgesteld en verspreid met het oogmerk om een protest te laten horen*. Dat hebben de personen achter de folder ook kenbaar gemaakt via internet (www.hetnieuwerijk.nl).
>
> Op basis hiervan zal/zullen de opsteller(s) of verspreiders van de folder niet strafrechtelijk worden vervolgd."[52]

Het Nieuwe Rijk reageerde hierop als volgt:

> "Het Nieuwe Rijk ziet het als een goed teken dat in onze democratie een tegengeluid betreffende het beleid van de overheid nog niet meteen tot vervolging leidt. Daarentegen heeft staatssecretaris Bijleveld laten zien dat zij de democratie niet zo hoog heeft zitten. Met de aangifte heeft zij geprobeerd een kritisch geluid tegen het overheidsbeleid de kop in te drukken en de makers van de folder te criminaliseren, naar de mening van Het Nieuwe Rijk zéér smakeloos.
>
> Door zonder juridische gronden aangifte te doen heeft zij de bevolking bewust misleid en de publieke opinie willen beïnvloeden om zodoende te proberen de discussie af te wenden van waar het werkelijk om gaat, namelijk de wijze waarop de overheid omgaat met haar burgers en hun privacy."[53]

Een dag nadat het OM had besloten niet tot vervolging te zullen overgaan, achtte de Reclame Code Commissie (RCC) de folder van Het Nieuwe Rijk echter in strijd met de Nederlandse Reclame Code (NRC). Allereerst achtte de RCC zich bevoegd, aangezien Het Nieuwe Rijk door middel van de folder "in feite het denkbeeld aan [zou prijzen] dat [de nieuwe Paspoortwet] dient te worden gewijzigd of ingetrokken"[54] en de RCC "bevoegd is *elke openbare aanprijzing van denkbeelden* te toetsen aan de Nederlandse Reclame Code."[55] Vervolgens achtte de RCC

de folder "onvoldoende *als reclame herkenbaar*, hetgeen in strijd is met artikel 11.1 NRC."[56] Ook zou Het Nieuwe Rijk zich in de folder niet als afzender hebben geïdentificeerd, hetgeen volgens de RCC in strijd was met artikel 2 van de Code Brievenbusreclame, Huissampling en Direct Response Advertising (CBR).[57] Verder oordeelde de RCC dat Het Nieuwe Rijk de Nieuwe Paspoortwet "niet in verband mag brengen met nazipraktijken *op de wijze zoals zij heeft gedaan*. De uiting is derhalve in strijd met artikel 2 NRC."[58] De uitspraken van de RCC zijn niet juridisch bindend. De RCC kon Het Nieuwe Rijk dan ook slechts adviseren "om niet meer op een dergelijke wijze *reclame* te maken."[59]

Terwijl het OM de folder van Het Nieuwe Rijk op 11 januari 2010 dus bestempeld had als een strafrechtelijk toegestane vorm van *protest*, bestempelde de RCC diezelfde folder een dag later als een verkeerde vorm van *reclame* (voor de denkbeelden van Het Nieuwe Rijk).

Het Nieuwe Rijk reageerde als volgt op de beslissing van de RCC:

> "Met een vergezochte beslissing wil de [RCC] acties als die van Het Nieuwe Rijk tegen de vingerafdrukkendatabank censureren. Recentelijk heeft de RCC de uitspraak van 12 januari jl. aan Het Nieuwe Rijk bekend gemaakt. Hierin heeft dit zelfregulerend orgaan bepaald dat de folders van Het Nieuwe Rijk, waarin wordt gesteld dat het mogelijk is om het Burger Service Nummer (BSN) op je arm te laten tatoeëren, onder de reikwijdte van de Nederlandse Reclame Code (NRC) zouden vallen. De RCC gaat daarmee voorbij aan het feit dat de actie een politiek doel had en daarom niet als reclame moet worden aangemerkt. Deze vergezochte redenering van de RCC probeert een politieke actie via het reclamerecht de kop in te drukken. Dit is des te opmerkelijker, nu het Openbaar Ministerie één dag eerder had besloten Het Nieuwe Rijk niet te vervolgen.
>
> Het Nieuwe Rijk heeft de tatoeagefolders verspreid om aandacht te vragen voor de aanleg van een databank met de vingerafdrukken van alle Nederlanders. De actie kreeg uitgebreid bijval in de media en via talloze e-mails, ook vanuit kringen van het voormalige verzet en de Joodse gemeenschap. De actie wordt ondersteund door bekende Nederlanders en burgerrechtenorganisaties. De petitie van Het Nieuwe Rijk om de wet terug te draaien is inmiddels door duizenden bezorgde Nederlanders ondertekend.
>
> Het Nieuwe Rijk verbaast zich dat de RCC oordeelt over deze actie, die een duidelijk politieke strekking heeft en het debat over het onderwerp wil aanwakkeren. Het verbieden van dergelijke acties is in strijd met de vrijheid van meningsuiting. De RCC gaat ook verder dan de beslissing [van] het Openbaar Ministerie, dat op 11 januari bepaalde dat Het Nieuwe Rijk niet zal worden vervolgd omdat er geen sprake is van een strafbaar feit.
>
> Als de bevoegdheid van de RCC en haar beslissingen leidend worden voor het beoordelen van politieke acties, zal deze uitspraak een verlammend effect hebben op het maatschappelijke debat. Het Nieuwe Rijk wil dit effect tegengaan, door de beslissingen van de RCC en het OM vanaf vandaag op haar website (www.hetnieuwerijk.nl) te publiceren."[60]

Het Nieuwe Rijk bereidt zich sindsdien op een volgende actie voor.

3.5 De nieuwe Paspoortwet wint een (drie)dubbele Big Brother Award

Ieder jaar worden door de digitale burgerrechtenbeweging Bits of Freedom[61] de zogenaamde Big Brother Awards uitgereikt: de prijzen voor de "grofste privacyschendingen"[62] van het

afgelopen jaar. Deze 'eer' viel de nieuwe Paspoortwet in essentie reeds ten deel in 2005, lang voordat de wet überhaupt het stadium van wetsvoorstel had bereikt:

> "In de categorie voorstellen is het Kabinetsvoornemen bekroond voor de centrale opslag van de biometrische gegevens die iedere Nederlander moet afstaan voor een nieuw paspoort (eerst een foto van het gezicht, later ook vingerafdrukken van de beide wijsvingers)."[63]

Het juryrapport motiveerde de uitreiking van deze Big Brother Award als volgt:

> "De jury is bezorgd over het voornemen biometrische gegevens centraal op te slaan. De doelstelling van het biometrisch paspoort verandert daarmee radicaal. De centrale opslag is een schoolvoorbeeld van wat ook 'function creep' wordt genoemd; de oorspronkelijke doelstelling wordt langzaam verschoven door het toevoegen van nieuwe functionaliteiten en dus ook nieuwe veiligheidsrisico's.
>
> Een centrale database met de vingerafdrukken en foto's van alle Nederlanders verhoogt de kans op misbruik aanzienlijk. De centrale database zal een aantrekkelijk doelwit zijn voor hackers binnen de georganiseerde misdaad omdat daarmee grootschalige identiteitsdiefstal mogelijk wordt. Een succesvolle aanval op de centrale database zou een nationale ramp betekenen.
>
> De centrale database van foto's opent op termijn bovendien de mogelijkheid cameratoezicht in het project te betrekken. Door middel van gezichtsherkenning is het dan mogelijk personen te identificeren en te volgen in hun bewegingen. Centrale opslag creëert dus een infrastructuur met potentieel zeer ernstige privacy-bedreigingen."[64]

Overigens was het voorstel voor biometrie in het paspoort ook al in 2004 genomineerd geweest (toen echter zonder een Award te winnen):

> "Nederland gaat een biometrisch paspoort invoeren met vingerafdrukken en een digitale foto. Het paspoort maakt het mogelijk om biometrische gegevens van Nederlanders op te slaan in centrale databanken. Ook valt te verwachten dat het biometrisch paspoort zal leiden tot een vloed aan identificatieverplichtingen in de private sector."[65]

En zelfs in 2002 stonden twee 'oudgedienden' van het biometrische paspoortproject al op de nominatielijst voor een Big Brother Award: minister Roger van Boxtel (D66) "voor het promoten van een algemene identificatieplicht en biometrie technologie" en CDA-Kamerlid Joop Wijn "voor het promoten van een vingerafdrukkendatabank voor alle inwoners van Nederland."[66]

Na 2007 leidde Bits of Freedom om financiële redenen enige tijd een slapend bestaan. Na de doorstart van Bits of Freedom halverwege 2009 viel de nieuwe Paspoortwet echter opnieuw in de prijzen, ditmaal zelfs dubbel: tijdens het Awardsgala op 5 februari 2010 ontving de wet zowel de Publieksprijs als de Big Brother Award in de categorie 'Overheid'. De Big Brother Award in de categorie 'Personen' ging naar minister Ter Horst van Binnenlandse Zaken (PvdA) "vanwege haar gevaarlijke gebrek aan nuance in het privacydebat. Mede door haar toedoen stevent Nederland in sneltreinvaart af op een controlemaatschappij, waar veiligheid

altijd boven persoonlijke vrijheid gaat."[67] Het oordeel van de jury over de nieuwe Paspoortwet luidde als volgt:

> "... Het bewaren van vingerafdrukken van alle Nederlanders op één plek vormt een ernstige privacyschending. Het risico op identiteitsfraude is substantieel. Centrale opslag maakt controle op de mate waarin en de voorwaarden waaronder de gegevens worden gebruikt, moeilijk zo niet onmogelijk; en een hack van de database heeft potentieel desastreuze gevolgen. De jury is zeer kritisch over de nieuwe wet, en constateert dat de Nederlandse overheid hiermee veel verder gaat dan de ons omringende landen.
> (...)
> Voorheen werd de vingerafdruk alleen afgenomen van verdachten. Nu belanden de vingerafdrukken van alle Nederlanders in een landelijk opsporingsregister. (...) Ondanks [de uitspraak van het EHRM in *Marper v. UK*], herhaaldelijke adviezen van het CBP, wetenschappers, privacywaakhonden, juristen en zelfs de Verenigde Naties negeert de overheid de bezwaren consequent. (...) Als de vingerafdrukken van alle burgers verzameld en op één plek bewaard worden, wordt met de databank een nieuwe goudmijn voor criminelen in het leven geroepen. Een vingerafdruk is eenvoudig te kopiëren, en met een nagemaakte vingerafdruk kan een slimme crimineel de illusie wekken dat iemand anders op een plaats delict is geweest. Zo wordt de politie op een dwaalspoor gezet, en een onschuldige burger verdacht. En als de centrale databank wordt gehackt, liggen al onze vingerafdrukken op straat en is forensisch onderzoek op basis van vingerafdrukken op plaatsen delict voorgoed onmogelijk geworden. Daarnaast vormt de aanleg van de databank de opmaat voor *function creep*: toekomstig gebruik van de vingerafdrukken voor andere doelen dan waarvoor zij oorspronkelijk verzameld zijn. (...) Het lijkt alsof de overheid amper heeft nagedacht over dit soort complexe, langetermijn-consequenties van centrale opslag."[68]

En over de verantwoordelijke minister:

> "... Door haar eenzijdige focus op vermeende functionaliteit en efficiëntie, en haar gebrek aan begrip voor het belang van privacybescherming, bouwt zij mee aan de instrumenten van een politiestaat. Tijdens haar korte bewind heeft de minister talloze wapenfeiten op haar naam gezet, die een nominatie voor een Big Brother Award verdienen. (...)
>
> Onder het bewind van minister Ter Horst is de opslag van vingerafdrukken in het kader van het biometrisch paspoort ingevoerd. Waar zij geregeld verwijst naar een verplichting die zou voortvloeien uit Europese regelgeving, bestaat die verplichting niet ten aanzien van de verzameling van twee extra vingerafdrukken en de centrale opslag daarvan in een landelijke databank. Ter Horst luistert niet naar kritiek over veiligheid (een beveiligingslek is mogelijk rampzalig), noodzaak (buurlanden hanteren minder ingrijpende oplossingen) en *function creep* (de Officier van Justitie krijgt toegang tot de vingerafdrukkendatabank), terwijl haar ministerie critici de mond snoert door aangifte te doen. (...) Ook stelde zij onlangs fier 'van de stroming veiligheid boven privacy' te zijn. Deze dooddoener komt haar op een bijzondere vermelding te staan.
>
> Met haar rigide standpunten simplificeert Ter Horst het debat over privacy. Ze polariseert door te suggereren dat wie niets te verbergen heeft, ook niets hoeft te vrezen, en te stellen dat veiligheid altijd boven privacy gaat. Volgens de Jury kunnen die twee in werkelijkheid niet zonder elkaar, en kan de categorie Personen niet zonder een nominatie voor minister Ter Horst."[69]

Minister Ter Horst en staatssecretaris Bijleveld waren tijdens het Awardsgala niet aanwezig om hun prijzen persoonlijk in ontvangst te nemen, maar reageerden wel schriftelijk:

> "Meestal als een prijs aan je wordt toegekend is dat een reden voor trots en blijdschap: je dankt – bij voorkeur met een brok in de keel – de jury of het publiek, je familie en iedereen die het heeft mogelijk gemaakt, dat je deze prijs in de wacht mocht slepen. Het zal u niet verbazen dat ik bij deze Big Brother Award gemengde gevoelens heb. Als verantwoordelijk minister voor

de AIVD behoor ik natuurlijk standaard tot de kanshebbers! Dit is niet het moment voor een diepgaande beschouwing, maar ik wil er toch kort iets over kwijt.

Laat ik dit voorop stellen: de sleutel tot succes van de bescherming van persoonsgegevens ligt ook bij een grotere bewustwording bij de burger. Zo lijkt bij jongere generaties privacy nauwelijks een rol te spelen in hun contacten op websites. Daarnaast is de politiek aan zet: de kern van politiek en van bestuur is het afwegen van belangen. En een gevolg daarvan is dat je het nooit iedereen naar de zin maakt. Als minister van Binnenlandse Zaken en Koninkrijksrelaties ben ik onder meer verantwoordelijk voor de Grondwet, maar ook – samen met mijn collega van Justitie – voor de veiligheid in ons land. Uitgerekend deze week voerden wij in de Tweede Kamer een discussie over de balans tussen veiligheid en privacy. In dat debat kregen minister Hirsch Ballin en ik waardering, zowel van de regeringspartijen als van de oppositie, over de manier waarop wij met die balans tussen veiligheid en privacy omgaan. En ik denk dat een representatieve steekproef onder alle Nederlanders een zelfde beeld zou opleveren.

De (publieks)jury denkt daar blijkbaar anders over. Toch waardeer ik uw initiatief en deze Award. Want ik vind het een goede zaak dat u ons scherp houdt als het om privacy gaat en dat u kritisch meekijkt bij wat we doen. Ik houd wel van tegengas, maar steek mijn eigen mening ook niet onder stoelen of banken. Laat van u horen, vooral ook richting de Tweede Kamer, want daar moet uiteindelijk beoordeeld worden hoe we in ons land met die balans moeten omgaan.”[70]

“De bezwaren die sommige mensen hebben tegen het centraal opslaan van vingerafdrukken zijn bekend. Deze bezwaren zijn uitvoerig aan de orde geweest en besproken in zowel de Tweede als de Eerste Kamer. Alle argumenten zijn gewisseld en in beide Kamers heeft een zorgvuldige afweging plaatsgevonden tussen het recht van de burger op de bescherming van zijn persoonlijke levenssfeer en het belang van de overheid om misbruik van reisdocumenten en de gevolgen van identiteitsfraude op een effectieve manier te kunnen bestrijden. In die afweging bleek de behoefte aan een centrale reisdocumentenadministratie zwaarder te wegen dan de inbreuk die dit maakt op de persoonlijke levenssfeer door de opslag van vingerafdrukken, foto en handtekening.”[71]

Aan de uitreiking van de Big Brother Awards werd uitgebreid aandacht besteed door de media.[72] Het evenement zelf was volgens de organisatie een groot succes:

“Na de uitreiking van de Big Brother Awards 2009 staat één ding als een paal boven water: ‘vrijheid is hot, controle is not’. Nog nooit ontving de jury zoveel kandidaten voor een nominatie vanuit het Nederlandse publiek. Nog nooit hebben alle winnaars (...) tijdens het uitverkochte Awardsgala gereageerd. En nog nooit behaalden de awards voor de grofste privacyschendingen zoveel publiciteit. Nederlanders hebben genoeg van de ongebreidelde controledrift waaraan zij worden onderworpen, en komen met een heldere boodschap: respecteer mijn privacy en laat vrijheid het uitgangspunt zijn van beleid. Bits of Freedom zal deze boodschap namens u allen uitdragen richting de overheid en het bedrijfsleven.”[73]

3.6 Utrechtse student begint bestuursrechtelijke procedure tegen opslag van vingerafdrukken

De eerste Nederlandse burger die zich met behulp van nationale rechtsmiddelen actief verzette tegen de nieuwe Paspoortwet, deed dit langs bestuursrechtelijke weg: op 15 februari 2010 tekende de 24-jarige Utrechtse student Aaron Boudewijn administratief beroep aan tegen het gemeentelijke besluit om hem geen geldig paspoort te verstrekken wegens zijn weigering om zijn vingerafdrukken en gezichtsscan in de reisdocumentenadministratie te laten opslaan. De beroepsprocedure van Aaron Boudewijn werd ondersteund door de

vereniging Vrijbit en aanhangig gemaakt bij de rechtbank Utrecht. De Volkskrant berichtte als volgt:

> "Zijn paspoort is verlopen. Een rijbewijs krijgt hij niet, om medische redenen. Als zijn bijna gebroken Europese identiteitsbewijs het begeeft, heeft hij niets meer waarmee hij zich nog kan identificeren. En gewoon een paspoort aanvragen? Dat heeft Aaron Boudewijn (24) gedaan, maar hij krijgt het niet. Want hij weigert zijn vingerafdrukken af te staan, en zonder vingerafdrukken krijgt hij geen paspoort. 'Ze mogen best mijn vingerafdrukken in mijn paspoort zetten, maar ik wil niet dat ze ze opslaan in een databank.'
>
> *Wat is daar mis mee?*
> 'Daarmee maakt de overheid inbreuk op mijn privacy. Ik wil niet als een potentiële verdachte in zo'n databank worden opgenomen. Bovendien zijn vingerafdrukken makkelijk na te maken, op YouTube vind je daarover allerlei filmpjes. Straks blijkt iemand met mijn gestolen vingerafdruk een misdrijf te begaan en kan ik niet bewijzen dat ik het niet was.'
>
> *Je had toch voor 21 september 2009, de dag dat de Paspoortwet in werking trad, een paspoort kunnen aanvragen?*
>
> 'Dat was ik ook van plan. Maar die week had ik Mexicaanse griep. En toen ik op 21 september een paspoort aanvroeg, weigerde de gemeente Utrecht de aanvraag te behandelen, tenzij ik mijn vingerafdrukken afgaf.'
>
> Intussen heeft hij bij de burgemeester bezwaar gemaakt tegen die weigering, en dat is verworpen. Maandag heeft hij tegen dat besluit beroep aangetekend bij de afdeling bestuursrecht van de rechtbank van Utrecht. Hij wordt bijgestaan door een advocaat en door de privacyorganisatie Vrijbit.
>
> *Hoe is het leven zonder paspoort?*
> 'Erg lastig. Ik ben lid van een Europese studentenorganisatie die veel activiteiten organiseert. De afgelopen maanden wilde ik naar bijeenkomsten in Azerbeidzjan, Servië en Rusland, maar dat kon dus niet. Binnen de Europese Unie en nog een paar landen kan ik met mijn identiteitsbewijs terecht, zolang dat nog niet gebroken is. Daarbuiten kan soms een noodpaspoort uitkomst bieden, maar dat kost 84,50 euro per keer, en veel landen kom je er nauwelijks mee in.'
>
> *En als je identiteitskaart breekt?*
> 'Dan kan ik geen rekening meer openen, geen arbeidscontract aangaan, geen huurovereenkomst, geen studiefinanciering aanvragen, niet meer stemmen. Ik kan niet naar het ziekenhuis, niet naar de dokter. Dus ik ben heel zuinig op mijn kaart. Hij zit nu in twee beschermhoesjes, maar als ik hem moet gebruiken, moet hij er altijd uit. Dan ben ik bang dat hij breekt, ik moet daar nog iets op vinden.'
>
> *Wat wordt dit voor procedure?*
> 'Ik denk dat deze zaak uiteindelijk bij het Europees Hof voor de Rechten van de Mens komt. Ik weet zeker dat ik uiteindelijk zal winnen.'"[74]

Aaron Boudewijn werd ook geïnterviewd op Radio 1.[75] In dezelfde uitzending werd staatssecretaris Bijleveld om een reactie gevraagd:

> Interviewer: "*Waar de tegenstanders natuurlijk bang voor zijn, is dat elke afzonderlijke politieman straks in dat archief kan gaan kijken.*
> [Bijleveld:] Ja, en dat mag niet, en dat gebeurt ook niet. (...) Onder de huidige Paspoortwet is het zo dat de officier van justitie al bepaalde gegevens mag gebruiken die vanuit die paspoorten zijn opgeslagen. Maar wat we nu hebben gedaan, is dat we juist heel strak in de wetgeving hebben aangegeven wie wat mag gebruiken, en *het mag nóóit voor strafrechtelijke opsporing worden gebruikt. Het mag alleen voor identiteitsvaststelling.*

> [Interviewer:] *Er zijn partijen die dat wel willen, hè? De PVV heeft bijvoorbeeld gezegd: gebruik die gegevens wel gewoon om…*
>
> [Bijleveld:] Maar ik wil dat niet. Kijk, dat is even helder: *ik wil dat niet, en deze regering wil dat niet.*
>
> [Interviewer:] *En als [de PVV] nou in een volgende regering [komt]?*
> [Bijleveld:] Ik heb ook in de Kamer gezegd, zowel in de Tweede als in de Eerste Kamer: ik weet natuurlijk nooit wat mensen na mij daarvan vinden, maar in alle gevallen moet dan de wet worden gewijzigd, en daar is de Tweede Kamer dan ook weer bij. Dus het kan niet zomaar. *Nu is het echt expliciet uitgesloten. Het mag niet [voor opsporing] gebruikt worden.* (…)”[76]

Aan het begin van de uitzending was aan de luisteraars de volgende stelling voorgelegd: “vingerafdrukken voor het nieuwe paspoort mogen in een databank worden opgenomen.” Aan het einde van de uitzending bleek 36% van de luisteraars het met deze stelling eens; 64% was het met de stelling oneens. Op dat moment hadden 2042 mensen via de website gestemd. Later was het aantal stemmers opgelopen tot 3763, waarvan 33% vóór en 67% tegen de stelling.[77] Overigens was enkele maanden eerder door hetzelfde radioprogramma een vergelijkbare stelling voorgelegd: “een database met vingerafdrukken uit ons paspoort schendt de privacy.” Destijds was 56% (van in totaal 2413 luisteraars) het met deze stelling eens; 44% was het oneens.[78] Deze cijfers duiden op een afnemend maatschappelijk draagvlak voor de opslag van vingerafdrukken in de reisdocumentenadministratie.

Op 14 april 2010 diende de advocaat van Aaron Boudewijn (mr. Marq Wijngaarden van advocatenkantoor BFKW) de gronden van het beroep in bij de afdeling bestuursrecht van de rechtbank Utrecht.[79] De zaak eindigde echter abrupt toen Aaron op 24 april 2010 thuis overleed aan de gevolgen van een epileptische aanval.[80] Een dag eerder had hij tijdens een congres over privacy in de Eerste Kamer nog een aantal parlementariërs toegesproken.[81]

Naar verwachting zou het bestuursrechtelijke traject door anderen worden voortgezet.

3.7 Zorgen over opslag van vingerafdrukken op gemeentelijk niveau

Ook op lokaal politiek niveau werd de opslag van vingerafdrukken aan de orde gesteld, allereerst in de Zaanstreek:

"Geacht college,

Graag ontvangen wij van u het antwoord op de volgende vragen:

Zijn de inwoners van Zaanstad ervan op de hoogte gesteld dat er een wettelijke verplichting is tot het afgeven van vingerafdrukken die op 21 september 2009 is ingegaan? Zijn de inwoners tevens op de hoogte dat de vingerafdrukken worden opgeslagen en door allerlei instanties kunnen worden geraadpleegd? Zo nee, bent u bereid de inwoners uitgebreid te informeren voor welke doeleinden deze gegevens worden opgeslagen?

Wat is de informatie die de gemeente Zaanstad geeft aan bewoners wanneer deze geen vingerafdrukken willen afgeven? Is het dan nog mogelijk om een paspoort of identiteitsbewijs te verkrijgen? En wat zijn de wettelijke mogelijkheden om tegen het afgeven van vingerafdrukken in beroep te gaan?

Hoe veilig is het systeem waarin de gegevens met betrekking tot de vingerafdrukken worden opgeslagen? Maakt de gemeente Zaanstad gebruik van een eigen of van een centraal opslagsysteem?

Hoe gaat de gemeente om met identiteitsfraude en hoe worden slachtoffers van identiteitsfraude door de gemeente Zaanstad bijgestaan?

Voor de spoedige beantwoording van de vragen danken wij u bij voorbaat.

Met vriendelijke groet,

Namens de SP-fractie

Roland van Braam".[82]

Binnen enkele dagen leidden deze vragen van het lokale SP-raadslid op het internet tot een spontane email-actie van burgers om andere gemeenteraadsleden in de rest van Nederland vergelijkbare vragen te laten stellen.[83] Dit gebeurde vervolgens onder andere in Purmerend, Amsterdam, Huizen en Nijmegen.[84] Een en ander sloeg daarna ook over naar politieke partijen in de Tweede Kamer.[85]

Begin maart 2010 werden de vragen door B&W van de gemeente Zaanstad als volgt beantwoord:

"... *Wanneer de gegevens centraal worden opgeslagen* en kunnen worden gebruikt door een beperkt aantal andere autoriteiten, instellingen en personen zullen wij de burgers van Zaanstad, in een brief die ze ontvangen enkele weken voordat het reisdocument gaat verlopen, informeren over het gebruik van vingerafdrukken.

(...) De medewerker van de afdeling Klantcontact Burgerzaken van de gemeente Zaanstad kan de burger die geen vingerafdruk wil afgeven niet helpen bij het aanvragen van een reisdocument. Het is niet mogelijk een paspoort of identiteitskaart aan te vragen zonder het afgeven van vingerafdrukken. Er is een wettelijk voorschrift waarvan niet kan worden afgeweken. Indien de burger toch een aanvraag wil doen wordt namens de burgemeester de aanvraag buiten behandeling gesteld. De aanvraag voor het reisdocument is immers niet compleet en de burger heeft nog de mogelijkheid een complete aanvraag in te dienen. *Het buiten behandeling stellen van een aanvraag is geen besluit* [*sic*]

Op de vraag of de burger nog wettelijke mogelijkheden heeft om tegen het afgeven van vingerafdrukken in beroep te gaan kunnen wij nu nog geen antwoord geven. Wij wachten onder meer de uitspraak van de rechter af die het beroep behandelt van de Utrechtenaar die

> een procedure startte bij de rechtbank Utrecht omdat hij weigerde zijn vingerafdrukken in de databank te laten opnemen.
>
> (...) Burgers die slachtoffer zijn van identiteitsfraude en contact opnemen met de gemeente Zaanstad worden doorverwezen naar het Centraal Meldpunt Identiteitsfraude (CMI). Slachtoffers van identiteitsfraude kunnen per 1 december 2008 terecht bij het Centraal Meldpunt Identiteitsfraude, dat is ondergebracht bij het Agentschap BPR. Hier worden gedupeerden ondersteund en geadviseerd."[86]

Dit leidde later tot een zitting van de gemeenteraad Zaanstad waarin een en ander prominent op de agenda stond en ook aan externe partijen gelegenheid tot inspraak werd geboden (onder andere Vrijbit maakte hier gebruik van).[87] Besloten werd om het thema op de agenda te houden. Een latere motie van de SP (gesteund door GroenLinks, Trots op Nederland en enkele kleine partijen) om "de minister van Binnenlandse Zaken garanties te vragen met betrekking tot de opslag van vingerafdrukken nu en in de toekomst" werd echter verworpen door een kleine meerderheid van CDA, VVD, PvdA en D66.[88]

Vrijwel identieke vragen als in Zaanstad waren in de gemeente Huizen gesteld door GroenLinks.[89] De beantwoording daarvan verschilde op enkele punten echter fundamenteel:

> "*Tegen het besluit tot het niet in behandeling nemen van een aanvraag voor een paspoort kan wel bezwaar worden ingediend*; in bezwaar zal dan worden beoordeeld of terecht is besloten de aanvraag niet in behandeling te nemen; indien die reden is dat de aanvrager geen vingerafdrukken wilde verstrekken zal het bezwaar ongegrond worden verklaard omdat het hier een wettelijke plicht betreft."[90]
>
> "Indien de gemeente fouten heeft begaan (verkeerde vingerafdruk in paspoort terecht gekomen, of gegevens gestolen bij gemeente door ontoereikende beveiliging), en die fouten worden de gemeente toegerekend door de rechter, zal de gemeente ook aansprakelijk zijn voor (een deel van) de schade. *Een dergelijke situatie zal mede door de verzekeraar moeten worden beoordeeld: indien ondanks de vereiste zorgvuldigheid bij het werkproces toch fouten zouden zijn ontstaan, dan zal dit onder de dekking van de gemeentelijke verzekering vallen.*"[91]

In Nijmegen waren vragen door de lokale D66-fractie gesteld over tal van kwesties, waaronder eventuele bezwaarprocedures en de verificatie van vingerafdrukken.[92] De burgemeester van Nijmegen (oud-minister voor Bestuurlijke Vernieuwing Thom de Graaf) antwoordde hierop dat inderdaad "[d]oor een aantal burgers is geïnformeerd naar de procedure van bezwaar maken."[93] De manier waarop met eventuele bezwaren zou worden omgegaan liet hij echter in het midden: "[b]ezwaren van burgers zullen op de binnen de gemeente Nijmegen afgesproken wijze worden afgehandeld."[94] Duidelijker was hij over de verificatie bij afgifte van het reisdocument:

> "In de standaardprocedure en de richtlijnen van het Ministerie van BZK is opgenomen dat alleen als er getwijfeld wordt aan de identiteit van de houder van het reisdocument een verificatie plaatsvindt. Als een klant vraagt om verificatie van de juistheid van de vingerafdruk wordt dit gehonoreerd. Voordat het document wordt uitgereikt aan de burger kan de verificatie op een eenvoudige wijze plaatsvinden."[95]

Tegelijkertijd had een brief van Vrijbit aan alle burgemeesters van Nederland inmiddels tot vragen van veel gemeenten richting de NVVB (en VNG) geleid:

> "10 mei jongstleden stuurde Vrijbit een brief aan alle burgemeesters in Nederland met het verzoek zelf, of in samenwerking met collega burgemeesters, zo spoedig mogelijk de rechter om hulp te vragen bij uitvoering van de Paspoortwet. De NVVB is inmiddels door veel gemeenten benaderd met een verzoek te adviseren in het opstellen van een reactie.
>
> Vrijbit roept burgemeesters op de rechter te vragen bevrijd te worden uit de onmogelijke positie waarin burgemeesters volgens Vrijbit, door loyale uitvoering van de Paspoortwet zijn geplaatst tegenover inwoners van gemeenten. In het bijzonder voor die inwoners voor wie de Paspoortwet onacceptabel is, stappen te zetten omdat Vrijbit meent dat burgemeesters een primaire zorgplicht hebben."[96]

Naar aanleiding van de brief van Vrijbit adviseerden de NVVB en VNG (na overleg met BZK) Nederlandse gemeenten enkele weken later als volgt:

> "De NVVB en VNG vinden dat de opname van vingerafdrukken in het reisdocument en de centrale opslag zorgvuldigheid vereist. Voor de uitvoerders is het van het grootste belang dat zij een integer proces doorlopen bij de verwerking van aanvragen voor reisdocumenten. VNG en NVVB vinden het van groot belang dat in dit proces door gemeenten kwaliteit geleverd kan worden. *Dit integere proces is dan ook een aantal malen onderwerp van bespreking geweest met het ministerie van BZK*. (...) Het Nederlandse parlement heeft, zoals u weet, met de wijziging van de Paspoortwet ingestemd. Daarmee is de Paspoortwet een wet die gemeenten in medebewind uitvoeren die op democratische wijze tot stand is gekomen en aan internationale rechtsnormen is getoetst. (...) Het is juist dat een besluit zorgvuldig tot stand dient te komen en deugdelijk is gemotiveerd, *waarbij het uiteindelijke oordeel daarover bij de rechter ligt*. Dit wil echter nog niet zeggen dat de burgemeester in de bezwaarschriftprocedure het werk van de wetgever over moet doen. (...) In het licht van het voorgaande adviseren de NVVB en VNG u bij aanvragen door personen die principiële bezwaren hebben tegen het opnemen van hun vingerafdrukken de volgende lijn aan te houden:
> (...)
> - het aanvoeren van principiële bezwaren tegen het opnemen van vingerafdrukken of de opslag daarvan in de reisdocumentenadministratie kan er niet toe leiden dat een reisdocument zonder vingerafdrukken wordt verstrekt (ook niet voor 1 jaar!). (...)
> - indien een aanvrager vanwege principiële bezwaren geen vingerafdrukken wil laten opnemen, moet u de bestaande procedure volgen. Die houdt in dat u de aanvraag, nadat betrokkene eerst nog in de gelegenheid is gesteld deze aan te vullen, niet in behandeling neemt. *Tegen dit besluit kan de aanvrager een bezwaarschrift indienen bij de burgemeester*. Indien de aanvrager in het bezwaarschrift stelt dat het besluit in strijd zou zijn met hogere wetgeving (bijvoorbeeld artikel 8 EVRM) kunt u het handhaven van het besluit om de aanvraag niet in behandeling te nemen uitdrukkelijk motiveren met een verwijzing naar de parlementaire geschiedenis van de gewijzigde Paspoortwet, waaruit blijkt dat daarbij een uitgebreide toetsing aan hogere wetgeving heeft plaatsgevonden.
>
> Wanneer u verdere adviezen nodig heeft over de afhandeling van de brief van Vrijbit adviseert de VNG en NVVB u contact op te nemen met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties."[97]

In dit advies zou impliciete (in bedekte termen gestelde) kritiek van de NVVB en VNG richting BZK kunnen worden gelezen met betrekking tot de kwaliteit van het proces van *enrolment* van vingerafdrukken. Verder wordt de principieel bezwaarde burger nadrukkelijk gewezen op de weg van bezwaar (bij de burgemeester) en beroep (bij de rechter).

3.8 Het recht in eigen hand: de GemeenteGarantieBrief

Eind maart 2010 ontwikkelde de stichting Privacy First[98] een zogenaamde 'GemeenteGarantieBrief'.[99] Door middel van deze modelbrief kunnen burgers bij het aanvragen van een nieuw paspoort de behandelende ambtenaar vragen om "zwart-op-wit te verklaren dat [hun] gemeente haar verantwoordelijkheid neemt voor de veiligheid van [hun] persoonlijke gegevens, zoals [hun] vingerafdrukken."[100] Volgens Privacy First bracht de nieuwe Paspoortwet voor burgers immers "ernstige en wellicht onnodige risico's voor de persoonlijke levenssfeer met zich mee waartegen zij zich niet kunnen wapenen."[101] Door wederzijdse ondertekening van de GemeenteGarantieBrief zouden burgers zichzelf kunnen indekken tegen de eventuele gevolgen van hoe door de overheid met hun gegevens zou worden omgesprongen. De NVVB en BZK reageerden als volgt:

> "De NVVB adviseert dringend, net als overigens het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, brieven van burgers gebaseerd op de standaardbrief van Privacy First, niet in ontvangst te nemen, laat staan deze te ondertekenen. De uitvoering van publiekrechtelijke taken, zoals op het terrein van de Paspoortwet, kan geen onderwerp zijn van een overeenkomst met een individuele burger."[102]

Dit leidde vervolgens tot enige aandacht in de media,[103] gevolgd door mondelinge vragen aan de staatssecretaris op initiatief van de PvdA (gevolgd door vragen van de SP, GroenLinks, CU, PvdD, CDA en het lid Verdonk):

> "De PvdA maakt zich zorgen over het draagvlak voor de Paspoortwet, die vorig jaar in werking is getreden. Het aantal berichten over verzet tegen het afgeven van vingerafdrukken, die sindsdien in het paspoort moeten worden opgenomen, neemt eerder toe dan af. Sommigen ervaren het afgeven van vingerafdrukken als een ingrijpende aantasting van hun privacy en integriteit. Actiegroepen en burgers maken zich zorgen over de veiligheid van de opslag van persoonsgegevens, in het bijzonder van vingerafdrukken."[104]

De staatssecretaris reageerde hierop als volgt:

> "Gemeenten hebben het ministerie vragen gesteld over een actie. Wij hebben daarop een advies gegeven. Er is geen sprake van een burgerbrief zoals de [PvdA] zegt, het gaat om een actie van de Stichting Privacy First. Deze stichting legt de gemeenten een verklaring voor over de opslag van vingerafdrukken en vraagt gemeenteambtenaren die te ondertekenen. Verder moeten zij aangeven hoe zij met vingerafdrukken omgaan en verklaren dat zij zich aan bepaalde garanties houden. Wij hebben gemeenten geadviseerd om die verklaring inderdaad niet in ontvangst te nemen, daarmee niets te doen en zeker niet te ondertekenen. Gemeenten moeten zich aan de wet houden. Zij hebben geen enkele ruimte in het kader van het opslaan van vingerdrukken. Wij hebben dat hier minutieus met elkaar besproken en bepaald. Het moet gebeuren zoals het in de wet is vastgelegd. Daarin zit geen enkele beleidsruimte voor hen. In die zin hebben wij gemeenten geadviseerd niet op de actie in te gaan en geen verklaringen te ondertekenen. (...) Wat staat er nu in die verklaring? Er wordt aan een gemeenteambtenaar gevraagd om een verklaring te ondertekenen waarin men zich op een bepaalde uitvoering vastlegt. Dat kan gewoon niet, want wij regelen die uitvoering hier centraal. (...) Een ander punt in de verklaring – dat is een buitenwettelijk punt – is de vraag om te verklaren dat men uitsluitend met toestemming van de burger vingerafdrukken uit de reisdocumentenadministratie verstrekt. Dat hebben wij niet geregeld in de wet, dus dat kan die ambtenaar ook niet verklaren. Wij hebben strak aangegeven wanneer iets wordt verstrekt, en daarbij is niet geregeld dat er toestemming moet zijn van degene die de vingerafdrukken

> geeft. Er staan in die verklaring dus allerlei buitenwettelijke zaken, en dat moet de gemeenteambtenaar niet ondertekenen."[105]

Er waren ook enkele andere opvallende, meer algemene passages in de beantwoording van de staatssecretaris:

> "De [PvdA] heeft gevraagd hoe ik aankijk tegen de voortdurende discussie. Wij hebben ons tijdens het debat allemaal gerealiseerd dat die discussie gevoerd zou worden. De veiligheid moet maximaal zijn. *Ik ben zeker bereid om daarover in gesprek te gaan met welk comité dan ook*. Ik ben ook bereid om met de gemeenten in gesprek te gaan over hun zorgen in dezen. Men heeft mij echter nooit om een gesprek gevraagd."[106]

> "De vraag hoe vaak mensen weigeren om vingerafdrukken af te geven, kan ik op dit moment niet beantwoorden. Iemand die dit weigert, kan dan ook geen paspoort krijgen."[107]

> "Bij het wetsvoorstel hebben wij uitgebreid gediscussieerd over de onrust. Ik ben toen uitgebreid ingegaan op de zorgen die de Kamer had. Ik heb uitgebreid aangegeven hoe ik kijk naar de beveiliging en naar de decentrale opslag – er is nog geen centrale opslag – van gegevens die er altijd al was. Ik heb aangegeven hoe het staat met de beveiliging en hoe belangrijk ik een goede beveiliging vind. Een vragenuurtje lijkt mij niet het moment om een algemene beschouwing te geven over het omgaan met gegevens en vingerafdrukken. Dat is bij de wet uitgebreid aan de orde geweest."[108]

> "Het is niet zo dat wij blind zijn, of horende doof voor wat zich in de samenleving afspeelt, maar wij hebben er alles aan gedaan om dit, gegeven dat wat vanuit Europees verband over ons komt, zo goed mogelijk te regelen."[109]

> "Deze opslag van vingerafdrukken en andere gegevens is iets wat we al jaren doen. Er is nog nooit een probleem geweest met die decentrale opslag."[110]

Tenslotte stelde het CDA nog de volgende vraag:

> "Zijn er na het debat dat wij ruim een jaar geleden hadden, nieuwe feiten of argumenten op tafel gekomen die rechtvaardigen dat er onrust of gebrek aan draagvlak zou zijn?"[111]

De staatssecretaris: "Het antwoord op die vraag is klip-en-klaar: nee."[112]

Een week na dit Kamerdebat zou oud-minister van Binnenlandse Zaken Ter Horst (PvdA) tijdens een evenement in Amsterdam echter publiekelijk verklaard hebben dat "criminaliteitsbestrijding naar haar mening de belangrijkste reden vormt voor de opslag van vingerafdrukken."[113]

In lijn met het eerdere BZK- en NVVB-advies terzake reageerde oud-minister voor Bestuurlijke Vernieuwing Thom de Graaf een maand later (als burgemeester van Nijmegen) als volgt op de actie van Privacy First:

> "De gemeente Nijmegen zal een op de door Privacy First opgestelde 'Modelbrief gemeentegarantie' gebaseerde verklaring niet innemen of ondertekenen. De uitvoering van publiekrechtelijke taken, zoals op het terrein van de Paspoortwet, kan namelijk geen onderwerp zijn van een overeenkomst met een individuele burger. Dit wordt ook geadviseerd door [BZK en de NVVB]."[114]

3.9 Kort geding tegen opslag van vingerafdrukken in Den Haag

Een tweede bestuursrechtelijke zaak werd in de zomer van 2010 geïnitieerd door de 26-jarige Louise van Luijk. Op 27 juli 2010 tekende zij beroep aan tegen het definitieve besluit van de burgemeester van Den Haag om haar geen paspoort te verstrekken wegens haar weigering om vingerafdrukken in de reisdocumentenadministratie te laten opslaan. Het buiten behandeling stellen van haar oorspronkelijke aanvraag van een nieuw paspoort dateerde van 8 februari 2010. Zij ging echter reeds sinds november 2009 zonder geldige identiteitsdocumenten (wegens vermissing en diefstal daarvan) door het leven; dit terwijl zij zwanger was. Deze situatie noodzaakte haar in mei 2010 tevergeefs tot het aanspannen van een kort geding:

> "Zelfs een kort geding, op 11 mei, met verzoek haar een tijdelijk nooddocument te verstrekken om als zwangere vrouw in aanmerking te kunnen komen voor reguliere medische hulp en om als moeder haar, inmiddels geboren dochtertje, aan te kunnen geven bij de burgerlijke stand, vond geen gehoor bij de voorzieningenrechter."[115]

Enkele eerste relevante overwegingen van de voorzieningenrechter[116] zagen op het spoedeisend belang van de zaak en op hetgeen niet tussen beide partijen in geschil was:

> "Verzoekster stelt spoedeisend belang te hebben bij deze procedure omdat zij rond 22 juli 2010 haar kind verwacht. Voor (eventuele) behandelingen in het ziekenhuis, voor de erkenning van het kind door de vader en voor de aangifte van het kind bij de burgerlijke stand dient zij in het bezit te zijn van een geldig identiteitsdocument. De voorzieningenrechter acht, gelet hierop, voldoende spoedeisend belang aanwezig.
>
> De voorzieningenrechter stelt vast dat tussen partijen niet in geschil is dat de bepalingen in de Paspoortwet verder gaan dan zijn voorgeschreven in de [Europese paspoort]verordening. De verordening draagt lidstaten op vingerafdrukken af te nemen en deze op te slaan in een interoperabel formaat, de verordening draagt niet op deze vingerafdrukken op te slaan in een (centrale) databank. Evenmin is tussen partijen in geschil dat de opslag van de vingerafdrukken in een (centrale) databank een inbreuk vormt op het recht [op] bescherming van de persoonlijke levenssfeer."[117]

Vervolgens verwees de voorzieningenrechter met name naar de memorie van toelichting bij de nieuwe Paspoortwet; dit echter zonder een en ander inhoudelijk aan het recht te toetsen.[118] Hierna luidde de kernoverweging van het vonnis als volgt:

> "Voor het treffen van een voorlopige voorziening als gevraagd zou slechts aanleiding kunnen zijn indien sterke twijfel bestaat aan de rechtmatigheid van het bestreden besluit en een zwaarwegend spoedeisend belang maakt dat het voor verzoekster onevenredig bezwaarlijk zou zijn de beslissing in de bodemprocedure te moeten afwachten. Van dusdanige omstandigheden is de voorzieningenrechter niet gebleken.
> Ter zitting heeft verzoekster nogmaals benadrukt dat het haar om een principiële kwestie gaat. De voorzieningenrechter is van oordeel dat de voorzieningen procedure zich niet leent voor een diepgaander toets van het recht. Mocht in een bodemgeschil, waar wél ruimte is voor deze diepgaander toets, blijken dat de regelgeving toch niet rechtmatig is dan zijn de gevolgen voor verzoekster omkeerbaar. Zij kan op grond van een zodanige uitkomst van een bodemgeschil een procedure starten met het doel haar vingerafdrukken uit de (centrale) database te laten verwijderen.

> De voorzieningenrechter overweegt, voorshands oordelend, dat de voorliggende regelgeving in de paspoortwet, gelet op hetgeen hiervoor (...) is uiteengezet met betrekking tot de wijze waarop de wetgever de in aanmerking te nemen belangen expliciet heeft afgewogen, niet onrechtmatig voorkomt. Derhalve is de voorzieningenrechter van oordeel dat verweerder verzoeksters aanvraag tot afgifte van een nationaal paspoort terecht buiten behandeling heeft gelaten."[119]

Inmiddels heeft Louise een eigen website gelanceerd: www.louisevspaspoortwet.nl

3.10 Civiele rechtszaak ter onrechtmatigverklaring van de nieuwe Paspoortwet

Op 8 december 2009 had stichting Privacy First[120] (bijgestaan door het advocatenkantoor SOLV) aangekondigd een civiele procedure tegen de Nederlandse staat te zullen beginnen indien de nieuwe Paspoortwet niet geheel of gedeeltelijk zou worden ingetrokken.[121] De eerste juridische stap daartoe was een schriftelijk verzoek van Privacy First aan minister Ter Horst. Daarna zou "onverbiddelijk het zwaard van Damocles [vallen]"[122]:

> "Middels een brief aan de Minister van Binnenlandse Zaken, heeft de stichting Privacy First vandaag haar onvrede geuit over de gewijzigde Paspoortwet.
>
> Privacy First is een stichting die zich inzet voor de bescherming van het recht op privacy. Naar de overtuiging van Privacy First is de nieuwe wet - met de (centrale) opslag van persoonsgegevens, zoals vingerafdrukken, in de zogenaamde reisdocumentenadministratie - onrechtmatig en dient deze geheel of gedeeltelijk buiten werking te worden gesteld.
>
> De opslag van persoonsgegevens is volgens Privacy First onder meer in strijd met art. 8 EVRM, de Privacyrichtlijn en de Wet bescherming persoonsgegevens.
>
> Privacy First heeft de Minister gesommeerd om voor 22 december te bevestigen dat zij bereid is in overleg te treden om de onrechtmatige situatie op te heffen. Als de minister niet aan deze sommatie voldoet, behoudt Privacy First zich het recht voor om rechtsmaatregelen tegen de Nederlandse Staat te treffen."[123]

"De tijd van kopjes thee met koekjes is voorbij", zo benadrukte Privacy First verder.[124] Eerder was de geplande rechtszaak door privacyjuristen al 'kansrijk' genoemd.[125] Een en ander werd door Privacy First als volgt toegelicht:

> "*Probleem*
> De Nederlandse regering wil de gewone en biometrische persoonsgegevens niet uitsluitend in het paspoort verwerken (...) maar wil daar ook zelf de volledige beschikking over krijgen door ze op te nemen in een digitaal overheidsregister (een database) waar alle gegevens van een ingezetene in kunnen worden vastgelegd. Zo'n opslag maakt een grote inbreuk op de bescherming van de persoonlijke levenssfeer. Niemand heeft meer zicht op a) waar zijn gegevens worden vastgelegd, b) wie er toegang toe heeft, c) wat ermee gebeurt. De gevaren zijn onder meer identiteitsdiefstal, identiteitsverwisseling, oneigenlijk gebruik van persoonsgegevens, verhandeling van persoonsgegevens aan buitenlanden of commerciële partijen, 'verlies' van gegevens of database, e.d. Een bijkomend probleem is dat als een burger daar buiten zijn schuld het slachtoffer van wordt, hij bij geen enkele overheidsinstantie verhaal kan halen. De wet stelt niemand verantwoordelijk voor schade of nadeel. Dit geheel betekent een forse afbraak van de *fundamentele burgerrechten* om in veiligheid en vrijheid te kunnen leven en onbespied en ongemoeid door het leven te kunnen gaan.

De gegevens worden momenteel met nagenoeg alle andere gegevens van iedere burger opgeslagen in zo'n 600 decentrale gemeentelijke databases. Deze gegevens kunnen op simpele manier in handen komen van goedbedoelende onbevoegden of kwaadwillende bevoegden, gestolen worden of gemanipuleerd worden – bijvoorbeeld uit politieke overwegingen of om eigen incompetentie of criminaliteit te verbergen – of tot chaos gehackt worden, bijv. door een boze ICT-medewerker.

De overschreden grens
De nieuwe Paspoortwet schendt ook een ander fundamenteel principe, namelijk dat iedereen geacht wordt onschuldig te zijn totdat hij veroordeeld is door een rechter. In de nieuwe opzet wordt iedereen als potentiële verdachte gezien. De Nederlandse samenleving is gebaseerd op waarden als tolerantie en vreedzame samenleving. De zeven provincies hebben rond 1575 Nederland opgericht op basis van vertrouwen en zo is het ook in 1848 door *Thorbecke* in de Grondwet opgeschreven die de grondvorm van de staatsinrichting vastlegde waarin wij *nog steeds* leven. De overheid herorganiseert de samenleving nu op basis van wantrouwen. Dat wetten dan *niet getoetst* mogen worden aan de Grondwet komt dan toevallig mooi van pas hoewel dat artikel daar niet voor was bedoeld.

Wilt u misschien in zo'n negatief gemanipuleerde samenleving leven? Privacy First en haar supporters in ieder geval niet.

De Paspoortwet maakt bovenstaande allemaal heel eenvoudig uit te voeren. De Paspoortwet overschrijdt de grens die niet overschreden had mogen worden. Daarom neemt Privacy First concrete en harde stappen om te voorkomen dat de Nederlandse samenleving straks met nog grotere invasies in het privéleven wordt geconfronteerd. Met 'hard' bedoelen wij dat als de verstandige rede van deskundigen, juristen en ICT-ers terzijde wordt geschoven om opportuun voordeel voor een heel kleine groep in Den Haag, Privacy First stappen zal nemen waar zelfs ministers of parlement niet omheen kunnen.

Vraag aan de lezer
Onze advocaat mr. Alberdingk Thijm zegt: 'Er is in Europa geen enkel ander land dat vingerafdrukken van zijn burgers in een centrale databank stopt.' Wij nodigen alle journalisten en iedere burger uit om als een detective te gaan uitzoeken waarom Nederland wel en anderen niet."[126]

Volgens Privacy First dreigt de centrale databank met vingerafdrukken een nationaal opsporingsregister te worden. "De database wordt onherroepelijk een nieuw speeltje van de politie die daar gaat rondneuzen naar vingerafdrukken. Maar ook buitenlandse mogendheden krijgen straks die mogelijkheid. Dat terwijl de controle van vingerafdrukken absoluut niet volledig betrouwbaar is."[127] Ook wordt het hierdoor "bijvoorbeeld een stuk makkelijker om iemand met behulp van valse vingerafdrukken een misdrijf in de schoenen te schuiven."[128]

Staatssecretaris Bijleveld leek zich over de rechtszaak weinig zorgen te maken: "De Eerste en Tweede Kamer hebben zich er al over gebogen. Ook is de wet niet in strijd met Europese regels", zo berichtte haar woordvoerder volgens de Telegraaf.[129] Nadat vervolgens tevergeefs overleg met BZK had plaatsgevonden,[130] werd na maanden van voorbereiding de Nederlandse staat op 6 mei 2010 door Privacy First en 22 mede-eisers (burgers) gedagvaard.[131]

Opvallend is dat de NVVB en VNG enkele maanden later (in een brief aan Vrijbit) als volgt aan de civiele rechtszaak van Privacy First refereerden:

> "Wij zijn van mening dat er tegen overheidsbesluiten zoals in casu aan de orde, een sluitend systeem van rechtsbescherming voor belanghebbenden bestaat. Wij denken dan ook dat de weg die door 'Privacy First' is ingeslagen, de juiste is. NVVB en VNG wachten daarom de uitkomsten van die bodemprocedure af."[132]

De conclusie van antwoord van de Nederlandse staat naar aanleiding van de dagvaarding door Privacy First wordt begin september 2010 verwacht.[133]

3.11 Intermezzo: *insiders* aan het woord

De geïnterviewde 'insiders' vonden de maatschappelijke kritiek op de nieuwe Paspoortwet over het algemeen te laat. In de woorden van Fons Knopjes:

> "Het idee voor een centrale database heeft een plek gekregen in de Paspoortwet. Dat is de Eerste Kamer gepasseerd en in principe is er dus geen beletsel meer om dit te gaan uitwerken. Dus dat er nu mensen zijn die meningen hebben die afwijken van de wet... Waar het wringt, is dat mensen dit denkproces pas opzetten nadat het besluitvormingsproces achter ons ligt. (...) De huidige maatschappelijke discussie is te laat. We hebben in 2004 in Brussel een besluit genomen, toen zat Nederland ook aan tafel. En nu is het de politiek voorbij, en nu gaat iedereen zeggen: 'ja, maar wacht eens even'. Dan had je in 2003 in Brussel moeten staan, toen het op de agenda kwam of in 2008/2009 toen het op de Nederlandse politieke agenda stond. Men heeft in algemene zin denk ik onvoldoende in de gaten hoe dat werkt. Ook bij de media. Ze volgen het gewoon niet."[134]

Bij Ruud van Munster klonk tevens verbazing over "de relatieve 'inertie' van het Nederlandse volk waar het dit soort thema's betreft; men lijkt zich er over het algemeen geen zorgen over te maken. Voor een deel is dit misschien ook te wijten aan het feit dat relevante maatschappelijke organisaties te lang achterover hebben geleund. Langzamerhand zijn daardoor veel mensen veiligheid belangrijker gaan vinden dan privacy. Sinds kort is er weliswaar weer een beetje discussie en protest in de maatschappij, maar het is nog maar de vraag hoeveel effect dit zal hebben."[135]

Dat de maatschappelijke discussie pas achteraf op gang kwam, was echter ook te wijten aan een gebrek aan transparantie van de overheid richting de burger, aldus Knopjes:

> "Waar het aan ontbreekt, is om het proces voor het voetlicht te brengen. Informatie is er in overvloed, maar het schort aan de communicatie en voorlichting van de overheid naar de burger toe. Vaak krijgen dingen zo een 'sneaky' karakter, terwijl dat helemaal niet de bedoeling is. Er is sprake van passiviteit bij de overheid om transparantie te benutten."[136]

Volgens Van Munster zou het hierbij vooral gaan om een gebrek aan transparantie vanuit agentschap BPR:

> "Een deel van de discussie en protesten hadden voorkomen kunnen worden als BPR vanaf het begin meer openheid van zaken zou hebben gegeven; e.e.a. komt deels voort uit het feit dat BPR dit dossier zo gesloten houdt. Die krampachtigheid van BPR werkt dus alleen maar averechts."[137]

Toch zou volgens Knopjes ruimschoots aandacht aan privacy besteed zijn, ook bij BPR:

> "In het hele traject rond de biometrische paspoorten en centrale opslag is 'privacy' volgens mij enorm aan bod gekomen. Voor een aantal mensen is het hun tweede natuur om daar constant mee bezig te zijn. Zeker ook binnen BPR."[138]

Opvallend is in dit verband de volgende passage uit notulen van het Nederlands Biometrie Forum (NBF) van eind 2008:

> "[Guus] Bronkhorst [BPR] geeft aan dat de aandacht voor privacy op dit moment politiek beperkt is, evenals de aandacht voor IT-infrastructuur, hoewel er volgens hem prangende vragen zijn over ordening en over hetgeen je vraagt aan de burgers als overheid."[139]

Daarentegen figureert een NBF-participant van Sagem in diezelfde notulen als volgt:

> "Van den Berg [Sagem] vraagt zich af of het niet hetzelfde kan gaan met biometrie als met de invoering van de pincode, namelijk geruisloos."[140]

Het "organiseren van je eigen kritiek" lijkt overigens een kunst apart te zijn, getuige de volgende passage uit het interview met Knopjes:

> "... je moet bijvoorbeeld een wet door de Kamer zien te krijgen, en dat betekent dat het uiteindelijk altijd via de politiek moet, dus in die zin maak je je geen illusies dat je ook dingen mist. Iets anders is: hoe komt dat hele spel tot stand? Heb je de juiste *governance* ingericht om zeker te weten dat je je omgeving goed mee hebt, heb je je kritiek goed georganiseerd, dat is heel belangrijk, dat je niet kort voor de besluitvorming te horen krijgt dat je een aantal dingen gemist hebt. Volgens mij zitten op dat terrein de dingen goed in elkaar."[141]

Wel was Knopjes in dit verband kritisch richting het CBP:

> "Het probleem met het CBP was dat ze nauwelijks betrokken wilden worden bij ontwikkeltrajecten en alleen hun mening wilden geven als e.e.a. voorlag ter politieke besluitvorming, op politiek opportune momenten. Het is natuurlijk hun goed recht dat ze zich niet willen verbinden aan ontwikkeltrajecten, maar voor de verantwoordelijke ontwikkelaar is het natuurlijk wel prettig als je in de ontwikkelfase de mening kunt krijgen van zo'n belangrijke instantie als het CBP. Als dat CBP voor dat soort doelen niet toegankelijk is, is dat natuurlijk niet goed. Het is niet erg als het CBP kritisch is, als het maar op het juiste moment is, en niet achteraf. Als je 'aan de voorkant mee instapt' kun je veel eerder zo'n signaal afgeven."[142]

Opvallend was verder dat er bij de NVVB geen zicht leek te zijn op de grootte van de groep principieel bezwaarden.[143] Hoewel het bestaan van deze groep tijdens het interview bij het ministerie van Buitenlandse Zaken wel werd erkend, bleek hier tegelijk het gebrek aan relevante keuzevrijheid:

> "We maken heel soms wel mee dat mensen geen vingerafdrukken willen afstaan. De instructies zijn in dat geval echter heel duidelijk: geen vingerafdrukken, geen paspoort. Vervolgens is de keuze aan de burger. Zo vertellen we het de burger ook."[144]

Vanuit het ministerie van Justitie klonk echter wel begrip voor de maatschappelijke kritiek:

> "Dat we biometrie bij gemeenten nodig hebben, dat staat buiten kijf. Maar dat we biometrie zo snel op een paspoort zetten in een vorm die heel fraudegevoelig is, dát is eigenlijk het drama. Het is nu nog veel te vroeg voor grootschalig gebruik van biometrie. Wat we nu aan het organiseren zijn, met die grootschalige toepassingen die heel onveilig worden, daarmee worden sociaal de kaarten verspeeld. Terwijl biometrie fantastisch is als technologie in kleine, gesloten groepen."[145]

3.12 Tussenconclusie

Van enig maatschappelijk debat over de nieuwe Paspoortwet was tot de zomer van 2009 vrijwel geen sprake. Dit lijkt met name te zijn veroorzaakt doordat de media amper aandacht aan het onderwerp besteedden, wat weer zou kunnen zijn veroorzaakt doordat de parlementaire ontwikkelingen terzake reeds sinds eind jaren 90 relatief geruisloos verlopen waren. Hierdoor zag het gros van de Nederlandse bevolking én het georganiseerde maatschappelijk middenveld zich in de zomer van 2009 plotseling gesteld voor een nationaal *fait accompli*: verplichte opslag van vingerafdrukken voor een ieder die graag nog eens op reis zou willen gaan, een bankrekening zou willen openen, een studie zou willen volgen, een arbeidscontract zou willen tekenen, een huis zou willen kopen, aan verkiezingen zou willen deelnemen of zelfs maar ongestraft (want identificeerbaar) over straat zou willen gaan.

Zodra de nieuwe Paspoortwet eenmaal was aangenomen leek de voorafgaande politieke en journalistieke stilte erover echter te werken als een maatschappelijke boemerang: waar een grondig en oprecht democratisch debat jarenlang *had* kunnen plaatsvinden, vond dit debat *alsnog* in versnelde, verhevigde en (mede daardoor) verjuridiseerde vorm plaats. Allereerst zette een brede coalitie van Nederlandse mensenrechtenorganisaties de nieuwe Paspoortwet vrijwel direct op de agenda van het VN-Mensenrechtencomité. De toon van het maatschappelijke debat over de nieuwe Paspoortwet was daarmee gezet en zou later worden aangevuld door een reeks aan kritische geluiden (en zelfs rechtszaken) van andere organisaties, juristen, wetenschappers, politici en activisten.

De algemene strekking van hun kritiek op de nieuwe Paspoortwet was (en is) dat door deze wet het recht op *privacy* van iedere Nederlander met voeten wordt getreden. Bovendien lijkt iedere Nederlander min of meer te worden gedwongen om zich daar bij neer te leggen: zonder geldig biometrisch identiteitsdocument zou men immers als het ware buiten de maatschappij worden geplaatst. Van enige vorm van *keuzevrijheid* (in menselijke zin) is in dit verband geen sprake. Voor de *identiteit* van principieel bezwaarden heeft de overheid vooralsnog geen oog. Het maatschappelijke proces dat hierdoor 'getriggerd' is heeft onlangs een eerste 'apotheose' bereikt in de vorm van een collectieve dagvaarding van de Nederlandse staat wegens vermeende schending van het recht op privacy. In die zin is de relatie tussen de burger en de Nederlandse overheid door het biometrische paspoort niet alleen reeds

veranderd, maar ook op scherp komen te staan, althans in juridische zin. In hoeverre dit eveneens geldt voor de andere beginselen in bredere, maatschappelijke zin zal in het volgende hoofdstuk blijken.

Noten

1 Dit op enkele uitzonderingen na, waaronder relevante items in RTL Nieuws (onder andere op 16 februari en 8 april 2008). Jaren eerder besteedde ook Zembla kritisch aandacht aan het biometrische paspoort (zie de uitzending van 11 november 2004: 'Code Oranje'). Nova wijdde er slechts één item aan, op 1 september 2006.

2 *Verzet tegen digitaal hamsteren; Eerste Kamer akkoord met Paspoortwet na verdediging door Bijleveld*, NRC Handelsblad, 10 juni 2009, p. 2. Zie tevens het hoofdredactioneel commentaar: *En weer een database*, ibid., p. 7.

3 *Maatschappelijk belang gaat bij paspoortwet voor de privacy*, Volkskrant, 12 juni 2009, p. 3.

4 Zie onder andere Annemarie Sprokkereef, *Men realiseert zich te laat hoe ingrijpend de nieuwe Paspoortwet is*, NRC Handelsblad, 20 juni 2009, Opinie, p. 10; *Met z'n allen in de databank van Vadertje Staat*, Groene Amsterdammer, 24 juni 2009; Ronald Leenes e.a., *Sla vingerafdrukken niet centraal op*, Volkskrant, 26 juni 2009, p. 9; Bart Jacobs e.a., *We vallen ten prooi aan Europese opslaghysterie*, Trouw, 26 juni 2009; *Vingerafdruk; de nieuwe paspoortwet*, Vrij Nederland, 27 juni 2009, p. 17. Zie ook *Nieuw paspoort met vingerafdrukken onveilig?*, Netwerk, uitzending 26 juni 2009. Tevens sprak CBP-voorzitter Jacob Kohnstamm zich in september 2009 nogmaals tegen de nieuwe Paspoortwet uit; zie *supra*, p. 105, noot 212.

5 Diverse belangengroeperingen hebben zich vervolgens aangesloten bij het nieuwe Platform Bescherming Burgerrechten; zie www.platformburgerrechten.nl. Dit Platform was in mei 2009 opgericht door het Humanistisch Verbond.

6 Zie www.njcm.nl/site.

7 In principe elke vijf jaar.

8 Zie UN Human Rights Committee, *Concluding Observations (Netherlands)*, UN Doc. CCPR/CO/72/NET (27 augustus 2001).

9 Zie *List of issues to be taken up in connection with the consideration of the fourth periodic report of the Netherlands*, UN Doc. CCPR/C/NLD/Q/4 (12 november 2008), par. 3.

10 NJCM *et al.*, *Addendum to the Commentary on the 4th periodic report of the Netherlands on the International Covenant on Civil and Political Rights (ICCPR)* (Leiden, 25 juni 2009), p. 1; beschikbaar op www.njcm.nl/site/treaty_reports/list. Zie voor meer informatie over het IVBPR en deze sessie van het VN-Mensenrechtencomité het persbericht van het NJCM: *Nederlandse mensenrechten onder de loep van de Verenigde Naties* (Leiden, 10 juli 2009); beschikbaar op www.njcm.nl/site/press_releases/show/25. Zie tevens www2.ohchr.org/english/bodies/hrc/hrcs96.htm en www.ccprcentre.org/en/home/82.

11 *Minister na kritiek op privacy: vingerafdruk wellicht weg uit paspoort*, NRC Handelsblad, 15 juli 2009, p. 3.

12 *Mensenrechtencomité zet vraagtekens bij hoeveelheid gevallen en procedure in Nederland*, Parool, 15 juli 2009.

13 UN Human Rights Committee, *summary record of the 2630*th *meeting, held at the Palais Wilson, Geneva, on Tuesday, 14 July 2009, at 3 p.m.* (UN Doc. CCPR/C/SR.2630 (30 november 2009)), par. 27; beschikbaar op www2.ohchr.org/english/bodies/hrc/hrcs96.htm. Zie tevens www.ccprcentre.org/en/home/82.

14 UN Human Rights Committee, *summary record of the 2631*th *meeting, held at the Palais Wilson, Geneva, on Wednesday, 15 July 2009, at 10 a.m.* (UN Doc. CCPR/C/SR.2631 (22 juli 2009)), par. 9; beschikbaar op www2.ohchr.org/english/bodies/hrc/hrcs96.htm. Zie tevens www.ccprcentre.org/en/home/82.

15 Zie bijvoorbeeld Max Snijder, Annemarie Sprokkereef en Ronald Leenes, *Wat wil Hirsch Ballin met de Paspoortwet?*, NRC Handelsblad, 24 juli 2009, p. 7.

16 Zie *Minister na kritiek op privacy: vingerafdruk wellicht weg uit paspoort*, *supra* noot 11; *Irisscan vervangt vingerafdruk*, Parool, 16 juli 2009, p. 4. De betreffende opmerking van de minister werd *en marge* van de VN-sessie gemaakt tegenover twee journalisten van NRC Handelsblad en het Nederlands Dagblad.

17 Telefonisch interview met minister Hirsch Ballin, BNR Nieuwsradio, 15 juli 2009, 06.41u.

18 Email van Nigel Rodley aan de auteur d.d. 1 februari 2010. De *Concluding Observations* van het VN-Mensenrechtencomité worden door consensus onder de Comitéleden bepaald; zie bijvoorbeeld Office of the United Nations High Commissioner for Human Rights, *Human Rights Fact Sheet No. 15 (rev.1) - Civil and Political Rights: The Human Rights Committee* (Genève, 2005), pp. 14, 19. Zie ook *Rules of procedure of the Human Rights Committee*, UN Doc. CCPR/C/3/Rev.8 (2005), p. 11 (noot bij *Rule 51*).

19 UN Human Rights Committee, *Concluding Observations (Netherlands)*, UN Doc. CCPR/C/NLD/CO/4 (30 juli 2009), par. 15; beschikbaar op www2.ohchr.org/english/bodies/hrc/hrcs96.htm.

20 Zie de brief van de minister van Justitie (Hirsch Ballin) d.d. 15 oktober 2009, *Kamerstukken II*, 2009-2010, 32123 VI, nr. 11.

21 Zie www.vrijbit.nl.

22 Vereniging Vrijbit, *Klacht over opslag van biometrische gegevens* (Utrecht, 2 augustus 2009); beschikbaar op www.vrijbit.nl/dossiers/dossier-vingerafdrukken/item/674-vrijbit-dient-klacht-in-tegen-nederlandse-staat; www.vrijbit.nl/media/k2/attachments/EVRM_klacht__8_2009_2.pdf.

---

23 *Vereniging tegen vingerafdrukken*, NRC Handelsblad, 14 augustus 2009, p. 2.

24 Brief van S. Quesada (griffier, 3e sectie EHRM) aan Vrijbit d.d. 24 augustus 2009, p. 1; www.vrijbit.nl/media/k2/attachments/24_8_09registratie_klacht_Hof_EHRMafwijzing_voorlopige_voorziening.pdf.

25 Zie Vrijbit, *Aangepast verzoek om voorlopige voorzieningen wegens onherstelbare schade veroorzaakt door schending van art. 8 EVRM*, Utrecht, 15 september 2009 (per fax); www.vrijbit.nl/media/k2/attachments/klachtEHRM15_09_2009.pdf.

26 *Opslag afdrukken onzeker*, Volkskrant, 16 september 2009, p. 5.

27 Zie fax van de griffie van het EHRM aan Vrijbit d.d. 18 september 2009; www.vrijbit.nl/media/k2/attachments/fax_ehrm.pdf. Deze (tweede) afwijzing van het spoedverzoek leidde in de Nederlandse media tot misleidende krantenkoppen als zou het hier om een definitief oordeel van het EHRM gaan; zie bijvoorbeeld *Archief vingerafdrukken mag*, Volkskrant, 19 september 2009; *Hof: vingerafdruk mag in databank*, NRC Handelsblad, 19 september 2009, p. 3. Zie voor vergelijkbare kritiek op dit misverstand K. Hermans, 'Het gebruik van vingerafdrukken voor opsporingsdoeleinden onder de nieuwe Paspoortwet en artikel 8 van het EVRM', *NJCM-Bulletin* 2010, pp. 36-37.

28 Vrijbit, *Hof weigert – zonder motivering – schorsing van opslag vingerafdrukken*, Utrecht, 18 september 2009; www.vrijbit.nl/dossiers/dossier-vingerafdrukken/nieuwsarchief-vingerafdrukken/item/710-hof-weigert-zonder-motivering-schorsing-van-opslag-vingerafdrukken.html.

29 Audioverslag NJCM-lustrumcongres '16 Miljoen BN'ers? Bescherming van Persoonsgegevens in het Digitale Tijdperk', Pulchri Studio Den Haag, 8 oktober 2009, fragment vanaf 1:01u.

30 *Verslag NJCM-lustrumcongres '16 Miljoen BN'ers? Bescherming van Persoonsgegevens in het Digitale Tijdperk'*, NJCM-Bulletin 34 (2009), nr. 8, pp. 949-950.

31 EHRM, *Vereniging Vrijbit v. The Netherlands*, Appl. No. 45692/09.

32 Schriftelijke vraag van Jeanine Hennis-Plasschaert (ALDE) aan de Commissie d.d. 5 augustus 2009, E-3962/09. Zie ook de toelichting van Hennis-Plasschaert op haar website: www.jeanineineuropa.nl/nieuws/nieuws_artikel.php?show=209 (21 juli 2009).

33 Zie Antwoord van de heer Barrot namens de Commissie d.d. 25 augustus 2009, E-3962/09.

34 Schriftelijke vraag van Jeanine Hennis-Plasschaert (ALDE) aan de Commissie d.d. 2 september 2009, E-4243/09. Zie ook de toelichting van Hennis-Plasschaert op haar website: www.jeanineineuropa.nl/nieuws/nieuws_artikel.php?show=215 (21 september 2009).

35 Antwoord van de heer Barrot namens de Commissie d.d. 29 september 2009, E-4243/09 (cursivering VB).

36 Schriftelijke vragen van Jeanine Hennis-Plasschaert (ALDE) aan de Commissie d.d. 8 en 13 oktober 2009, E-4811/09 en E-4867/09.

37 Antwoord van de heer Barrot namens de Commissie d.d. 10 december 2009, E-4811/09 en E-4867/09 (cursivering VB).

38 Jeanine Hennis-Plasschaert in Amnesty International's *Wordt Vervolgd*, nr. 5 - mei 2010, p. 9; beschikbaar op www.humanistischverbond.nl/nieuws/archief/2010/iedereenverdacht.

39 De folder had als titel 'Nieuw reisdocument aangevraagd?' en leek qua vormgeving sprekend op de folder die het ministerie van Binnenlandse Zaken in september 2009 nationaal verspreid had (zie *supra*, p. 107, noot 309). Afzender van de folder was 'Het Nieuwe Rijk' ("Gaat verder dan u denkt"). Zie voor een foto van de folder www.hetnieuwerijk.nl/media/FOLDER-overzicht.jpg.

40 Zie ibid.

41 Zie www.hetnieuwerijk.nl/index.php.

42 *Tatoeagefolder is actie tegen vingerafdrukkendatabase*, Het Nieuwe Rijk, 24 november 2009, 15.30u; www.hetnieuwerijk.nl/persberichten.php.

43 Ibid.

44 Zie voor een overzicht www.hetnieuwerijk.nl/media.php.

45 Zie Centrum Documentatie en Informatie Israel (CIDI), *'Rijksfolder' polstatoeage wekt angst en woede*, 24 november 2009; www.cidi.nl/index.php?option=com_content&task=view&id=584&Itemid=1.

46 Zie in eerste instantie *Misleidende folder over tatoeëren burgerservicenummer*, persbericht ministerie van Binnenlandse Zaken, 24 november 2009, www.minbzk.nl//onderwerpen/persoonsgegevens-en/reisdocumenten/nieuws--en/@123876/misleidende-folder.

47 Zie *Staatssecretaris doet aangifte over folder*, persbericht ministerie van Binnenlandse Zaken, 24 november 2009, www.minbzk.nl/actueel?ActItmIdt=123889.

48 Zie voor een overzicht www.hetnieuwerijk.nl/media.php.

49 *De tatoeagefolder was precies in de roos*, NRC Handelsblad, 1 december 2009, Opinie, p. 7.

50 Persbericht Het Nieuwe Rijk, 24 november 2009, 18.00u; www.hetnieuwerijk.nl/persberichten.php.

51 Persbericht Het Nieuwe Rijk, 26 november 2009; www.hetnieuwerijk.nl/persberichten.php

52 *Vervolgingsbeslissing OM 11 januari 2010*, gepubliceerd door Het Nieuwe Rijk op www.hetnieuwerijk.nl/persberichten.php (cursivering VB). Zie tevens *Folder tatoeëren BSN-nummer niet strafbaar*, persbericht ministerie van Binnenlandse Zaken, 12 januari 2010; www.minbzk.nl//onderwerpen/persoonsgegevens-en/reisdocumenten/nieuws--en/@124999/folder-tatoeeren; *Makers tatoeagefolder niet vervolgd*, Volkskrant, 12 januari 2010, p. 2.

53 Persbericht Het Nieuwe Rijk, 11 januari 2010, 19.00u; www.hetnieuwerijk.nl/persberichten.php.

54 Reclame Code Commissie, *X te Rotterdam v. Het Nieuwe Rijk*, 2009/00865, 12 januari 2010, p. 2.

55 Ibid (cursivering VB).

56 Ibid (cursivering VB).

57 Zie ibid.

58 Ibid., p. 3 (cursivering VB).

59 Ibid (cursivering VB).

60 *Reclame Code Commissie poogt vingerafdrukactie te censureren*, Het Nieuwe Rijk, 8 februari 2010; www.hetnieuwerijk.nl/persberichten.php. Zie voor overige reacties bijvoorbeeld '*Reclame Code Commissie censureert vingerafdrukactie*', Security.nl, 8 februari 2010.

61 Zie www.bof.nl.

62 Bits of Freedom, *Het is nu officieel: 'Vrijheid is hot, controle is not'*, 8 februari 2010, www.bigbrotherawards.nl/?p=547.

63 Big Brother Awards 2005, www.bigbrotherawards.nl/?page_id=13.

64 Ibid. De jury bestond onder meer uit advocaat Christiaan Alberdingk Thijm, hoogleraar computerbeveiliging Bart Jacobs (Radboud Universiteit Nijmegen), hoogleraar regulering van technologie Bert-Jaap Koops (Universiteit van Tilburg) en publiciste en Bits of Freedom-voorzitter Karin Spaink (juryvoorzitter).

65 Big Brother Awards 2004, www.bigbrotherawards.nl/index_2004.html.

66 Big Brother Awards 2002, www.bigbrotherawards.nl/index_2002.html.

67 Bits of Freedom, *Vijf Big Brother Awards én Winston Award uitgereikt*; www.bigbrotherawards.nl/?p=491.

68 Bits of Freedom, *Juryrapport Genomineerden Big Brother Awards 2009* (Amsterdam, januari 2010), pp. 9-11; beschikbaar op www.bigbrotherawards.nl/?page_id=359.

69 Ibid., pp. 35-37. De jury bestond ditmaal uit publiciste en voormalig Bits of Freedom-voorzitter Karin Spaink (juryvoorzitter), hoogleraar computerbeveiliging Bart Jacobs (Radboud Universiteit Nijmegen & Technische Universiteit Eindhoven), hoogleraar media- en telecommunicatierecht Nico van Eijk (Universiteit van Amsterdam), dr. Bart Schermer (Universiteit Leiden), hoogleraar ICT en sociale verandering Valerie Frissen (Erasmus Universiteit Rotterdam & TNO) en Bart de Koning (redacteur bij HP/De Tijd).

70 *Reactie minister Ter Horst op Big Brother Award*, 5 februari 2010; www.bigbrotherawards.nl/?p=515.

71 *Reactie staatssecretaris Bijleveld op Big Brother Award*, 5 februari 2010; www.bigbrotherawards.nl/?p=515.

72 Zie voor een overzicht www.bigbrotherawards.nl/?page_id=336.

73 Bits of Freedom, *Het is nu officieel: 'Vrijheid is hot, controle is not'*, *supra* noot 62.

74 '*Vingerafdrukken zijn makkelijk na te maken*', Volkskrant, 16 februari 2010, p. 3. Zie ook *Student klaagt Staat aan*, NRC Handelsblad, 17 februari 2010, p. 2; Folkert Jensma, '*Eerste vingerafdruk-weigeraar is voorbode van breder protest*', 17 februari 2010, http://weblogs.nrc.nl/rechtenbestuur/2010/02/17/eerste-vingerafdruk-weigeraar-is-voorbode-van-breder-protest; *Eerste weigeraar vingerafdruk; student vecht paspoortdatabank aan*, NRC Handelsblad, 18 februari 2010, p. 2; Marjolein Februari, *Natuurlijk is brutaliteit niet verboden, maar Bolkestein gaat wel heel ver*, Volkskrant, 20 februari 2010, p. 33.

75 Zie *Interview met Aaron Boudewijn*, Radio 1, 16 februari 2010; beschikbaar op www.radio1.nl/contents/12920-aaron-boudewijn-weigert-vingerafdruk-in-paspoort?autostart=15535.

76 *Interview met staatssecretaris Bijleveld*, Radio 1, 16 februari 2010, 13.15u (cursivering VB); beschikbaar op www.radio1.nl/contents/12926-vingerafdrukken-voor-paspoorten-mogen-in-een-databank-worden-opgenomen?autostart=15543.

77 Zie ibid., 13.30u. Zie tevens www.stand.nl/archief (stelling van 16 februari 2010).

78 Zie www.stand.nl/archief (stelling van 21 september 2009).

79 Zie www.privacynieuws.nl/nieuwsoverzicht/binnenlands-nieuws/politiek-en-overheid/4145-beroepsgronden-in-de-zaak-over-weigering-paspoort.html Het beroepsschrift spitste zich toe op art. 8 EVRM.

80 Zie Vrijbit, *In memorandum Aaron Boudewijn*, www.vrijbit.nl/dossier/registratie/dossier-paspoortwet/item/778-in-memorandum-aaron-boudewijn.html; *Voorvechter privacy overleden*, Volkskrant, 27 april 2010, p. 12; Bits of Freedom, *In Memoriam Aaron Boudewijn*, 26 april 2010, https://www.bof.nl/2010/04/26/in-memoriam-aaron-boudewijn.

81 Zie *Voorvechter privacy overleden*, *supra* noot 80.

82 *SP stelt vragen over opslag vingerafdrukken*, SP Zaanstreek, 16 februari 2010; beschikbaar op http://zaanstreek.sp.nl/bericht/41746/tw. Zie ook http://sp-politiek.hyves.nl/blog/31625906/vinger_afdruk_paspoort/UH_A/.

83 Zie onder andere *Schriftelijke vragen over vingerafdrukken hebben landelijk effect*, SP Zaanstreek, 22 februari 2010; beschikbaar op http://zaanstreek.sp.nl/bericht/42131/100222-schriftelijke_vragen_over_vingerafdrukken_hebben_landelijk_effect.html.

84 Zie *SP stelt vragen over vingerafdrukken*, SP Purmerend, 27 februari 2010, beschikbaar op http://purmerend.sp.nl/bericht/42453/100227-sp_stelt_vragen_over_vingerafdrukken.html; *Informeer Amsterdammers over vingerafdrukken*, SP Amsterdam, 15 maart 2010, beschikbaar op http://amsterdam.sp.nl/nieuws/berichten.php?itemid=3579; *Vragen van D66 over de evaluatie van de invoering van de vingerafdrukken in de Nijmeegse reisdocumentenadministratie RAAS*, D66 Nijmegen, 1 april 2010, beschikbaar op www2.nijmegen.nl/mmbase/attachments/924502/Vragen_-_Evaluatie_vingerafdrukken_RAAS.pdf; *Vragen GroenLinks over het opslaan van vingerafdrukken*, GroenLinks Huizen, 26 mei 2010, beschikbaar op http://huizen.groenlinks.nl/nieuws100526.

85 Zie pp. 85-86 *supra*.

86 Brief van B&W Zaanstad aan de gemeenteraad d.d. 4 maart 2010, kenmerk Z/2010/49354 (cursivering VB); beschikbaar via http://bis.zaanstad.nl/infoman/. Zie tevens de beantwoording van aanvullende vragen van de SP d.d. 16 april 2010 (over bestuurlijke toetsing aan Europees recht en civiele aansprakelijkheid van de gemeente).

87 *SP agenda initiatief opslag vingerafdrukken*, SP Zaanstreek, 12 april 2010, beschikbaar op www.zaanstreek.sp.nl/bericht/43857/100412-sp_agenda_initiatief_opslag_vingerafdrukken.html.

88 Zie gemeenteraad Zaanstad, motie 19 van SP e.a. over vingerafdrukken d.d. 17 juni 2010; beschikbaar via http://bis.zaanstad.nl/infoman/.

89 Zie *Vragen GroenLinks over het opslaan van vingerafdrukken*, GroenLinks Huizen, 26 mei 2010, *supra* noot 84.

90 Brief van B&W Huizen aan de fractie GroenLinks d.d. 23 juni 2010, p. 2 (cursivering VB); beschikbaar op http://huizen.groenlinks.nl/nieuws100526.

91 Ibid., p. 4 (cursivering VB).

92 Zie *Vragen van D66 over de evaluatie van de invoering van de vingerafdrukken in de Nijmeegse reisdocumentenadministratie RAAS*, D66 Nijmegen, 1 april 2010, *supra* noot 84. Zie voor andere onderwerpen die hierbij aan de orde kwamen (waaronder beveiligingsmaatregelen, de opleiding en certificering van gemeentelijk baliepersoneel en het inhuren en screenen van uitzendkrachten) het parallelle WRR-deelonderzoek van Max Snijder, WRR Casestudie: Black Box Biometrisch Paspoort (nog te verschijnen).

93 Th.C. de Graaf, *Antwoorden op vragen over de invoering van vingerafdrukken in de Nijmeegse reisdocumentenadministratie*, Nijmegen, 27 mei 2010, par. 5.; beschikbaar op www2.nijmegen.nl/mmbase/attachments/941636/Antwoord_-_Evaluatie_vingerafdrukken_RAAS.pdf.

94 Ibid.

95 Ibid., par. 6.

96 NVVB, *Vrijbit en burgemeesters in Nederland*, 21 mei 2010; beschikbaar op www.nvvb.nl/websites/nvvb/website/show.asp?Propid=1&ModuleType=news&path=gwsitemanager/content/show/421&newstype=8. Zie voor de betreffende brief van Vrijbit www.vrijbit.nl/persberichten/item/776.html.

97 NVVB & VNG, *Reactie brief Vrijbit aan burgemeesters*, 4 juni 2010 (cursivering VB); beschikbaar op www.nvvb.nl/websites/nvvb/website/show.asp?Propid=1&ModuleType=news&path=gwsitemanager/content/show/426&newstype=8.

98 Zie www.privacyfirst.nl.

99 De betreffende brief is (met gebruikersinstructie) beschikbaar op www.privacyfirst.nl/index.php/onze-focus/flankactie-gemeentegarantie-paspoort.

100 Homepage www.privacyfirst.nl, 31 maart 2010.

101 Ibid.

102 NVVB, *Stichting Privacy First en vingerafdrukken*, 2 april 2010; www.nvvb.nl/websites/nvvb/website/show.asp?Propid=327&ModuleType=news&path=gwsitemanager/content/show/403&newstype=8.

103 Zie bijvoorbeeld *Protest vingerafdrukken strandt in bureaucratie*, De Pers, 19 april 2010; *BZK adviseert gemeenten: negeer vingerafdrukbrief*, Webwereld, 19 april 2010.

104 Vragenuur, *Handelingen II*, 2009-2010, TK 78, 6605 (20 april 2010).

105 Ibid., 6605-6606.

106 Ibid., 6605 (cursivering VB).

107 Ibid.

108 Ibid., 6606.

109 Ibid.

110 Ibid., 6607.

111 Ibid.

112 Ibid.

113 Discussie tijdens het symposium 'De burger in de knel' in verband met de presentatie van Frank Kuitenbrouwers *Recht & Vrijheid*, 28 april 2010 te Amsterdam, als weergegeven in de dagvaarding van stichting Privacy First versus de Nederlandse staat d.d. 6 mei 2010, *infra* noot 131, p. 7.

114 Th.C. de Graaf, *Antwoorden op vragen over de invoering van vingerafdrukken in de Nijmeegse reisdocumentenadministratie*, Nijmegen, 27 mei 2010; beschikbaar op www2.nijmegen.nl/mmbase/attachments/941636/Antwoord_-_Evaluatie_vingerafdrukken_RAAS.pdf. Vergelijk het advies van BZK en NVVB *supra* noot 102. Zie voor de oorspronkelijke vragen van de Nijmeegse D66-fractie d.d. 1 april 2010 noot 84 *supra*.

115 Persbericht *Beroepsprocedure Louise vs. Paspoortwet*; zie www.louisevspaspoortwet.nl (28 augustus 2010).

116 De betreffende voorzieningenrechter was mw. Gisèle van Zeben-de Vries. (Sinds 2000 is zij tevens actief bij de VVD (partijcommissie politie, Den Haag). Voorheen (sinds 1988) was zij officier van justitie.)

117 Voorzieningenrechter rechtbank Den Haag 18 mei 2010, LJN: BM6929, rechtsoverwegingen 6.1-6.2; beschikbaar op www.rechtspraak.nl/ljn.asp?ljn=BM6929.

118 Zie ibid., rechtsoverwegingen 6.3-6.4.

119 Ibid., rechtsoverweging 6.6.

120 Zie www.privacyfirst.nl.

121 Privacy First had haar intentie om een proces te beginnen reeds maanden eerder breed kenbaar gemaakt; zie Privacy First, *Actie Paspoortwet in nieuwe fase*, Amsterdam, 2 oktober 2009; www.privacyfirst.nl/index.php/nieuwe-paspoortwet/309-actie-veiliger-paspoort-a-betere-paspoortwet; Privacy First, *Actie Paspoortwet: route gekozen*, Amsterdam, 14 oktober 2009; www.privacyfirst.nl/index.php/nieuwe-paspoortwet/312-paspoortwetactieroute-gekozen; *Vingerafdruk in het geding*, De Pers, 4 november 2009, pp. 1, 3; *Rechtszaak wegens vingerafdrukkendatabank*, NRC Handelsblad, 4 november 2009; *Proces tegen Staat over vingerafdrukdatabank*, Webwereld, 4 november 2009.

122 Privacy First, *Juridische procedure tegen paspoortwet gestart*, Amsterdam, 9 december 2009.

123 *Privacy First betwist rechtmatigheid wijziging Paspoortwet*, weblog advocatenkantoor SOLV, 8 december 2009; www.solv.nl/weblog/privacy-first-betwist-rechtmatigheid-wijziging-paspoortwet/16649.

124 Zie '*De tijd van thee en koekjes is voorbij*', De Pers, 11 december 2009, p. 6.

125 Zie '*Proces tegen Staat kansrijk'; centrale opslag vingerafdrukken kan struikelblok worden*, De Pers, 13 november 2009, pp. 1, 3.

126 Privacy First, *Slag om Nieuw Paspoort – verduidelijking*, Amsterdam, 15 december 2009; www.privacyfirst.nl/index.php/nieuwe-paspoortwet/352-paspoortkwestie-verduidelijking.

127 *Ter Horst voor de rechter; organisatie eist stopzetten registratie vingerafdrukken*, Telegraaf, 13 december 2009, p. 4; www.telegraaf.nl/binnenland/5560248/__Ter_Horst_voor_de_rechter__.html.

128 Ibid.

129 Ibid.

130 Zie voor een verslag www.privacyfirst.nl/index.php/paspoortwetproces/369-verslag-meeting-bzk-20-jan-2010 en p. 36 van de dagvaarding *infra* noot 131.

131 De tekst van de dagvaarding d.d. 6 mei 2010 is beschikbaar op www.privacyfirst.nl/index.php/onze-focus/actie-paspoortwet-2009. Zie tevens *Rechtszaak om vingerafdruk voor paspoort*, Telegraaf, 6 mei 2010; *Staat aangeklaagd om vingerafdrukdatabase*, Webwereld, 6 mei 2010, http://webwereld.nl/nieuws/65919/staat-aangeklaagd-om-vingerafdrukdatabase.html; Joyce Hes (voorzitter Platform Bescherming Burgerrechten), *Privacy First eist ongeldig verklaren Paspoortwet*, 6 mei 2010, beschikbaar op www.platformburgerrechten.nl/artikelen/2010/privacy_first_dagvaardt_staat.

132 NVVB & VNG, *Antwoord op brief Vrijbit aan NVVB en VNG van 18 juni 2010*, 4 augustus 2010, Zoetermeer.

133 De behandeling van deze zaak namens de Nederlandse staat zou overigens in handen zijn van Cécile Bitter (advocaat bij Pels Rijcken & Droogleever Fortuijn; tevens lid van het NJCM).

134 WRR-interview Knopjes, *supra* tabel 1.1, p. 3.

135 WRR-interview Van Munster, *supra* tabel 1.1, p. 4.

---

136 WRR-interview Knopjes, *supra* tabel 1.1, p. 6.
137 WRR-interview Van Munster, *supra* tabel 1.1, p. 4.
138 WRR-interview Knopjes, *supra* tabel 1.1, p. 5.
139 Verslag van het NBF-diner voor Senior-participanten d.d. 24 november 2008 te Utrecht, p. 1.
140 Ibid.
141 WRR-interview Knopjes, *supra* tabel 1.1, p. 6.
142 Ibid., p. 4.
143 Zie bijvoorbeeld WRR-interview Van Troost, *supra* tabel 1.1, p. 5.
144 WRR-interview Provily & Van der Zanden, *supra* tabel 1.1, p. 5.
145 WRR-interview Grijpink, *supra* tabel 1.1, p. 5.

4 EINDCONCLUSIES

Doel van dit onderzoek was om na te gaan op welke wijze invulling wordt gegeven aan een aantal fundamentele concepten die de relatie tussen de Nederlandse overheid en de burger in de moderne informatiesamenleving schragen, in het bijzonder in de context van het biometrische paspoort. De focus lag hierbij op de beginselen privacy, identiteit, transparantie, *accountability*, keuzevrijheid, effectiviteit en efficiëntie. Zowel ten aanzien van deze beginselen als ten aanzien van de bijbehorende verantwoordelijkheden van de Nederlandse overheid zullen hieronder een aantal conclusies worden getrokken.

4.1 Privacy

In algemene zin valt allereerst op dat in de loop van de parlementaire geschiedenis van de nieuwe Paspoortwet (die in wezen tot 1997 teruggaat) van overheidswege steeds minder aandacht aan het concept privacy *als zodanig* is besteed. Zo was er eind jaren 90 van regeringszijde nog sprake van een relatief breed scala aan relevant geachte juridische instrumenten en werd ook de Registratiekamer (het latere CBP) structureel bij een en ander betrokken. Dit echter in tegenstelling tot de Tweede Kamer (met name het CDA) van destijds, waar een geloof in biometrie reeds de overhand leek te hebben boven aandacht voor het recht op privacy van de burger. Tekenend in dit verband was het voorstel van het CDA (eind 2001) om de vingerafdrukken van alle Nederlanders via opname in het paspoort op te slaan voor opsporingsdoeleinden. Dit voorstel werd destijds echter door zowel de meeste andere politieke partijen als door de relevante minister naar de prullenbak verwezen, met name gezien het disproportionele karakter ervan.

Ook in de jaren na 2001 had de overheid in eerste instantie nog enig oog voor de privacy van haar burgers. Zo blijkt uit een onderzoeksrapport van BZK (agentschap BPR) uit 2003 dat “om redenen van privacybescherming” was afgezien van proeven met biometrische identificatie door middel van opslag van gegevens in een database. Na een serie bijeenkomsten tussen de VS en de EU trad vanaf eind 2004 echter een belangrijke kentering op: vanaf dit moment leek privacy meer en meer ondergeschikt te worden gemaakt aan belangen van veiligheid en terrorismebestrijding. Na de totstandkoming van de Europese paspoortverordening kondigde de Nederlandse regering begin 2005 aan te zullen overgaan tot centrale opslag van biometrische gegevens. Hieruit vloeide uiteindelijk de nieuwe Paspoortwet voort.

In de recente parlementaire geschiedenis van het biometrische paspoort lijkt zowel door de meeste politieke partijen als van regeringszijde op relatief oppervlakkige wijze aandacht te zijn besteed aan de privacy van de burger. Bij de nieuwe Paspoortwet stelde men zich collectief ten doel om (vrijwel ongekwantificeerde) *look-alike* fraude te gaan bestrijden en dit

primaire doel heiligde blijkbaar de middelen, inclusief grootschalige, amper beproefde middelen waarvan algemeen werd toegegeven dat die een inbreuk op de privacy van alle burgers zouden maken. Van regeringszijde (en ook door de PvdA-fractie) werd hierbij voornamelijk aangevoerd dat van grote veranderingen in de bestaande juridische situatie (inclusief opsporing en vervolging) geen sprake zou zijn, en dat *daarom* de privacy voldoende gewaarborgd zou zijn. Van schending van het recht op privacy zou verder geen sprake zijn omdat de algemene doelen van de nieuwe Paspoortwet nauwkeurig zouden zijn geformuleerd. Ook werd relevante Straatsburgse jurisprudentie door de verantwoordelijke staatssecretaris eenvoudigweg niet van toepassing geacht. De veiligheid van centrale opslag werd van regeringszijde met name *gesteld*, maar nauwelijks parlementair bediscussieerd en vervolgens onaangetoond gelaten. Ook werd het risico van *function creep* door de staatssecretaris grotendeels ontkend; dit terwijl dit risico uit de voorstellen en suggesties van sommige politieke partijen (waaronder de PVV en het CDA) reeds zeer groot bleek, met name in het kader van opsporing en vervolging.

Aan diverse risico's voor de privacy (waaronder RFID-technologie en internationale uitwisseling van biometrie) werd in de parlementaire debatten geen aandacht besteed en enkele hoofddoelen van de nieuwe Paspoortwet (waaronder wettelijke identificatie, rampenbestrijding en inlichtingenwerk) bleven zelfs vrijwel geheel onbesproken. Deze stilte heerste ook buiten het parlement, met name in de media. Zodra de nieuwe Paspoortwet was aangenomen werd de burger hierdoor dan ook als het ware overrompeld en middels een onvolledige overheidsfolder voor een *fait accompli* gesteld. Dit heeft vervolgens geleid tot een groeiende hoeveelheid protest vanuit de samenleving. Vanuit privacy-oogpunt kan men dan ook concluderen dat het biometrische paspoort de relatie tussen de burger en de overheid vooralsnog op scherp heeft gezet en naar alle waarschijnlijkheid het onderwerp van meerdere rechtszaken zal worden. Dit tenzij de nieuwe Paspoortwet voortijdig zal worden ingetrokken, opgeschort of parlementair zal worden herzien.

4.2 Transparantie

Evenals bij privacy lijkt de aandacht van de overheid voor transparantie op het terrein van het biometrische paspoort in de loop der jaren structureel te zijn afgenomen. Zo leek er eind jaren 90 nog sprake te zijn van relatieve openheid over alle (overheids)actoren die bij de ontwikkeling van het biometrische paspoort betrokken waren. Hoewel de betreffende belangen van deze actoren reeds in die vroege periode buiten beeld bleven, verkreeg de burger althans enig zicht op 'het veld en de spelers'. Ook werd men ingelicht over de betrokkenheid van buitenlandse instituten en over externe onderzoeken en *pilots*, waaronder een onderzoek naar de eigen besluitvorming. Geen van deze onderzoeken werd echter

(volledig) openbaar gemaakt, waardoor de burger afhankelijk bleef van wat de regering op basis van een en ander meende te kunnen concluderen. Ook was er weinig zicht op relevante private, industriële partijen (al werden Johan Enschedé, SDU en de bancaire sector wel uitdrukkelijk genoemd).

Een structureel gebrek aan transparantie bleek vervolgens uit de onderzoeksrapporten van agentschap BPR uit 2003 en 2005: onderliggende studies, proeven, *pilots* en primaire onderzoeksresultaten over biometrie en *look-alike* fraude waren veelal niet openbaar en leken qua resultaten positiever te zijn voorgesteld dan ze in werkelijkheid waren. Hetzelfde gold voor onderzoeken naar het maatschappelijk draagvlak voor biometrie van destijds.

Dit gebrek aan transparantie gold (en geldt) ook op internationaal en Europees niveau: voor de burger was en is het volstrekt onduidelijk wat zich op het terrein van biometrie afspeelt bij ICAO, de EU en de Raad van Europa alsmede tussen de VS, de EU en Nederland onderling (en de industriële lobby daaromheen), laat staan dat de burger zijn of haar eigen overheid of andere overheden hierop kan (laten) aanspreken. Hetzelfde geldt voor het EFTD/IF4TD: een intergouvernementeel forum waar zelfs experts niet van op de hoogte blijken.

Op nationaal niveau is het de laatste jaren niet beter gesteld: in de recente parlementaire geschiedenis van de nieuwe Paspoortwet blijft volstrekt onbekend welke binnen- en buitenlandse partijen bij een en ander betrokken zijn en wat hun belangen daarbij (geweest) zijn. Van enige kwantificering van *look-alike* fraude was evenmin sprake. Hetzelfde geldt voor een aantal hoofddoelen van de nieuwe Paspoortwet die tijdens de parlementaire behandeling vrijwel onbenoemd werden gelaten, waaronder binnen- en buitenlandse staatsveiligheid, terrorismebestrijding, rampenbestrijding en de uitvoering van wettelijke identificatieplichten. Verder dient de nieuwe Paspoortwet nog grotendeels te worden uitgewerkt onder het niveau van de wet in formele zin, terwijl de verantwoordelijke staatssecretaris vooraf geen toezeggingen heeft willen doen om het parlement bij de opstelling van de betreffende AMvRB's te betrekken. Aldus tast zelfs het Nederlandse parlement (weliswaar verwijtbaar) in het duister over tal van cruciale zaken. Intussen proberen verantwoordelijke bewindspersonen zich te verschuilen achter 'Brussel' en laten zij de precieze Nederlandse rol in het eerdere Europese proces onbenoemd.

Terwijl de nieuwe Paspoortwet relatief geruisloos door beide Kamers werd geloodst, heerste ook in de media stilte. Nadat de wet vervolgens (zonder stemming) was aangenomen door de Eerste Kamer, werd de Nederlandse burger alsnog 'geïnformeerd' middels een overheidsfolder die aan volledigheid veel te wensen overliet. Ook nu nog hebben de meeste

burgers geen idee voor welke doeleinden hun biometrische gegevens kunnen worden gebruikt.

Van alle beginselen (op keuzevrijheid na) lijkt transparantie in dit dossier door de overheid op de meest gebrekkige wijze te zijn ingevuld. Primair is het dan ook aan diezelfde overheid om alsnog openheid van zaken te verschaffen, bijvoorbeeld door relevante rapporten, onderzoeken, adviezen, departementale stukken en verslagen van internationale bijeenkomsten openbaar te maken. Dergelijke openheid van zaken zou tevens door politici, wetenschappers, journalisten en procederende burgers kunnen worden afgedwongen.

4.3 *Accountability*

In het verlengde van het gebrek aan transparantie op het terrein van het biometrische paspoort ligt het gebrek aan *accountability* terzake (en vice versa). De politieke verantwoordelijkheid voor de ontwikkeling van het biometrische paspoort lag achtereenvolgens bij de staatssecretaris van Binnenlandse Zaken, de minister voor Grote Steden- en Integratiebeleid, de minister voor Bestuurlijke Vernieuwing en (weer) bij de staatssecretaris van Binnenlandse Zaken. Eind jaren 90 zou er nog sprake zijn van afstemming van de juridische aspecten van het biometrische paspoort met de Registratiekamer (het latere CBP). Later zou tevens onderzoek zijn gedaan naar het draagvlak onder de bevolking en naar de eigen besluitvorming. Zoals eerder beschreven werden veel departementale onderzoeken, studies, proeven en *pilots* echter nooit (volledig) openbaar gemaakt en bleven participerende organisaties (zeker na de jaren 90) in toenemende mate buiten beeld. In die zin was en is er van effectieve *accountability* dan ook geen sprake; men kan immers niet goed worden aangesproken op dat wat onbekend is. Daartoe dienen tenminste eerst de feiten op tafel te komen. Hier lag een schone taak voor het parlement (en voor de media); een taak die echter grotendeels werd verzaakt. In informationele zin is er dan ook niet alleen sprake van een gebrek aan *accountability* op het niveau van verantwoordelijke bewindspersonen, maar ook op het niveau van het parlement zelf. Jarenlang werden al te kritische Kamervragen immers vermeden, werd over onderzoeken en *pilots* geen openheid van zaken geëist, liet men zich tijdens Kamerdebatten regelmatig met een kluitje in het riet sturen en werden complete delen van de nieuwe Paspoortwet zelfs onbesproken gelaten. Zo bezien lijkt hier dan ook sprake te zijn (geweest) van een dubbel (of zelfs driedubbel) democratisch tekort: 1) bij gebrek aan openbare informatie hoefden bewindspersonen zich tegenover het parlement amper over relevante zaken te verantwoorden, en 2) tegelijkertijd werden diezelfde bewindspersonen door het parlement nauwelijks gedwongen om informatie te verstrekken, terwijl 3) de media (op enkele uitzonderingen na) deze situatie jarenlang lieten voortduren. Behalve op nationaal niveau

geldt deze *accountability gap* nog sterker op Europees niveau (EU, Raad van Europa) en op internationaal niveau (ICAO). Een voorbeeld hiervan is het EFTD/IF4TD dat in enkele vroege Kamerstukken ten tonele verscheen, maar dat vervolgens voorgoed achter de departementale coulissen leek te zijn verdwenen.

Behalve door het gebrek aan actieve informatieverstrekking (en de parlementaire afdwinging daarvan), bleek een tekort aan *sense of accountability* voor het biometrische paspoort ook door het feit dat van regeringszijde nauwelijks werd ingegaan op de risico's van eventueel misbruik, onjuist en onvoorzien gebruik en de technische onvolkomenheden die aan grootschalige toepassing van biometrie inherent zijn. Ook kon men geen antwoord geven op de vraag of centrale opslag van biometrische gegevens veiliger zou zijn dan decentrale opslag en werd de kwestie van overheidsaansprakelijkheid in geval van een *data breach* of biometrische identiteitsfraude bewust onbeantwoord gelaten. Tegelijkertijd werd wel erkend dat biometrische identiteitsfraude iemand zijn leven lang kan blijven achtervolgen en onherstelbare schade teweeg kan brengen. Een belangenafweging tussen centrale of decentrale opslag (met centrale verwijsindex) werd echter pas na zware kritiek van het CBP opgenomen in de memorie van toelichting bij de nieuwe Paspoortwet. Overige (vrijwel unaniem negatieve) adviezen van relevante Nederlandse en Europese toezichthouders en experts werden structureel gebagatelliseerd of zelfs geheel genegeerd. Na inwerkingtreding van de nieuwe Paspoortwet bleek vervolgens ook een (vanuit agentschap BPR geïnstrueerd) gebrek aan *accountability* op gemeentelijk niveau, aangezien daar veelal geen sprake is van verificatie van de vingerafdrukken bij uitgifte van het reisdocument. Bovendien worden burgers actief ontmoedigd om bezwaar te maken tegen opslag van hun biometrische gegevens. Dergelijk bezwaar zou niet mogelijk zijn, hoewel hiertoe procedureel wel degelijk mogelijkheden bestaan.

De aanname van de Paspoortwet en de daaropvolgende maatschappelijke bewustwording en politiek-juridische activering zouden ertoe kunnen leiden dat de Nederlandse overheid alsnog gedwongen wordt om rekenschap over het biometrische paspoort en de centrale opslag van biometrie af te leggen. In die zin lijkt er sprake te zijn van een maatschappelijke inhaalrace ter compensatie voor het algehele gebrek aan *accountability* terzake van de laatste jaren. In eerste instantie blijft het echter aan de overheid zelf om de benodigde verantwoordelijkheid te betrachten, bijvoorbeeld door relevante informatie openbaar te maken, door open te staan voor externe adviezen, risico's en bijbehorende aansprakelijkheden te erkennen en door burgers te wijzen op hun rechten van biometrische verificatie, inzage, correctie en eventuele mogelijkheden van bezwaar.

4.4 Effectiviteit en efficiëntie

In de parlementaire geschiedenis kwamen de beginselen effectiviteit en efficiëntie vooral impliciet (en nauwelijks bediscussieerd, laat staan publiekelijk aangetoond) in beeld als zijnde inherent aan de (beleids)doelen die voor de invoering van het biometrische paspoort achtereenvolgens werden genoemd: modernisering en betere beveiliging van het paspoort, elektronische identificatie, bestrijding van (*look-alike*) fraude, betere (elektronische) dienstverlening aan de burger en geautomatiseerde identiteits- en grenscontrole. Op een vroeg voorstel van het CDA (in 2001) na was tot enkele jaren geleden van eventuele strafrechtelijke doelen in het geheel nog geen sprake.

Reeds in 1998 was gesteld dat de toepassing van biometrie mogelijkheden zou bieden om de beveiliging van reisdocumenten te verhogen. Men ging er vanuit dat hierdoor tevens een meer effectieve, betrouwbare verificatie van iemands identiteit zou kunnen plaatsvinden en dat daardoor ook *look-alike* fraude beter bestreden zou kunnen worden. Destijds werd echter tevens onderkend dat biometrie in de praktijk nog nauwelijks grootschalig was beproefd. Latere *pilots* bevestigden de bruikbaarheid van biometrie ter verbetering van identiteitscontrole aan de hand van reisdocumenten. Op basis *daarvan* achtte men biometrie tevens een geschikt middel ter bestrijding van *look-alike* fraude (maar dus zonder dit daadwerkelijk in de praktijk te hebben getest). Hetzelfde geldt voor later, gecontroleerd laboratorium- en literatuuronderzoek. Ook de gemeentelijke biometrieproef '2b or not 2b' had een volstrekt gecontroleerde opzet met vooraf geselecteerde vrijwilligers. Bij deze proef bleek bovendien dat er sprake was van een flinke foutmarge, zeker waar het de verificatie van biometrie (met name vingerafdrukken) betrof. Verder werden er geen harde cijfers en statistieken over identiteitsfraude (inclusief *look-alike* fraude) bekendgemaakt. Desalniettemin werd besloten om te kiezen voor invoering van de vingerscan in reisdocumenten (en gelaatsherkenning voor internationale grenspassage) met als primair doel de bestrijding van *look-alike* fraude.

Opvallend in de wetsgeschiedenis van het biometrische paspoort is tevens het grote verschil in gebruiksdoelen tussen het (nooit in werking getreden) wetsvoorstel van 2002 en de nieuwe Paspoortwet van 2009: terwijl in 2002 nog slechts sprake leek van *verificatie* van het reisdocument door middel van decentraal (gemeentelijk) opgeslagen biometrie, werd in 2009 de wettelijke basis gelegd voor *identificatie* door middel van centrale opslag (in een nationale database) voor meerdere doeleinden, waaronder ook opsporing en vervolging. Een aantal van deze nieuwe doeleinden bleven parlementair vrijwel onbesproken, wat vragen oproept over de democratische controle terzake. Ook lijkt men zich nooit te hebben afgevraagd of een centrale, online raadpleegbare database met de biometrische gegevens van 16 miljoen

Nederlanders op termijn niet juist tot (veel) meer identiteitsfraude en andere problemen zou kunnen leiden, hetzij van binnenuit (door inherente technische onvolkomenheden en foutmarges, menselijke corruptie of datalekken), hetzij van buitenaf (*hacking*). In dit verband dient verder te worden benadrukt dat uit eerder onderzoek in opdracht van agentschap BPR reeds was gebleken dat ook de toekomstige (door de nieuwe Paspoortwet in te voeren) plaatsonafhankelijke aanvraag en uitgifte van reisdocumenten tot meer identiteitsfraude zou kunnen gaan leiden, aangezien kwaadwilligen voortaan zouden kunnen gaan 'shoppen' bij gemeenten waar men het gemakkelijkst aan reisdocumenten zou kunnen komen. Tegelijkertijd blijkt *look-alike* fraude met Nederlandse reisdocumenten de laatste jaren reeds een relatief kleinschalig fenomeen te zijn geweest. Deze constateringen roepen dringende vragen op over de algehele effectiviteit en efficiëntie van de nieuwe Paspoortwet. Hetzelfde geldt voor het biometrische paspoort als middel voor terrorismebestrijding, aangezien terroristen meestal authentieke reisdocumenten gebruiken. Dit nog afgezien van het feit dat het hier in wezen buitengewoon kostbare symptoombestrijding betreft en dat over de (bestrijding van de) oorzaken van terrorisme vrijwel geen politieke discussie heeft plaatsgevonden.

Zoals elk grootschalig ICT-project van de overheid zou ook de ontwikkeling van het biometrische paspoort gebaat zijn geweest bij een goede interdepartementale samenwerking, onderlinge informatieverstrekking en externe advisering. In dit kader klonken met name kritische geluiden over de rol van agentschap BPR (BZK). Verder blijkt de biometrie op het paspoort te zijn ingevoerd zonder dat tevens de bijbehorende controle-infrastructuur (bijv. bij grenspassage) is ontwikkeld en zonder dat de biometrische gegevens bij uitgifte van het document worden geverifieerd. In die zin zou men de ontwikkeling van het biometrische paspoort tot nu toe kunnen beschouwen als een vorm van kapitaalverspilling.

4.5 Keuzevrijheid

In de vroege parlementaire geschiedenis van het biometrische paspoort bleek door de verantwoordelijke bewindspersonen nog de nodige waarde te worden gehecht aan de maatschappelijke acceptatie van biometrie. In die zin leek er destijds dus nog sprake te zijn van enige keuzevrijheid in ruime, collectieve zin aan de kant van de bevolking. In latere jaren raakte dit type keuzevrijheid echter in toenemende mate aan erosie onderhevig, getuige het feit dat er in parlementaire discussies steeds minder aandacht aan werd besteed. Dit zou echter ook verklaard kunnen worden door de snelle ontwikkeling die de biometrische techniek na '9/11' wereldwijd doormaakte, waardoor de maatschappelijke invoering van deze techniek volgens velen iets onvermijdelijks kreeg. Andere stuwende krachten gingen achtereenvolgens uit van het Amerikaanse *Visa Waiver Program* en van de (weliswaar mede

door Nederland tot stand gebrachte) Europese paspoortverordening. Op internationaal en Europees niveau was hierdoor ook voor de Nederlandse staat steeds minder sprake van keuzevrijheid waar het de invoering van biometrische paspoorten betrof. Dit liet de keuzevrijheid van Nederland inzake de eventuele opslag van de biometrische gegevens uit diezelfde paspoorten echter onverlet. Desondanks besloot Nederland – tegen vrijwel alle adviezen in – tot centrale opslag in een nationale database. In dit opzicht zou Nederland in toenemende mate een uitzonderingspositie kunnen gaan innemen binnen Europa.

Voor het Nederlandse parlement was bovendien sprake van een gebrek aan keuzevrijheid vanwege het feit dat de nieuwe Paspoortwet een zogenaamde 'nationale kop' op Europese implementatiewetgeving vormde. Beide Kamers werden hierdoor als het ware voor het blok gezet om deze (voor veel Kamerleden relatief onduidelijke) mix van Europese en nationale wetgeving als biometrische 'package deal' te aanvaarden.

Aan keuzevrijheid op het niveau van de individuele burger werd in de loop van de parlementaire geschiedenis steeds minder aandacht besteed. Van regeringszijde werd dergelijke keuzevrijheid geheel onwenselijk geacht, aangezien het een effectieve bestrijding van identiteitsfraude zou bemoeilijken. Ook zou de Europese paspoortverordening er geen ruimte toe bieden. Dit heeft geresulteerd in de huidige situatie waarin de burger op dit terrein in wezen geen enkele keuzevrijheid meer heeft, noch in maatschappelijke, noch in rechtsstatelijke zin. Immers: gemeenten zijn door de centrale overheid geïnstrueerd om bezwaren van principiële weigeraars niet in behandeling te nemen, en zonder geldig biometrisch identiteitsdocument wordt men tegenwoordig als het ware buiten de maatschappij geplaatst. Verder is de invoering van een alternatief identiteitsdocument zonder biometrie (voor binnenlands gebruik) tot nu toe geen onderwerp van serieuze politieke discussie geweest. Dit terwijl de overheid met een dergelijk document aan de bezwaren van deze groep mensen tegemoet zou kunnen komen, wat tevens een deel van de maatschappelijke onrust zou kunnen wegnemen. Hetzelfde geldt voor het standpunt van de overheid dat burgers niet tegen de opslag van hun biometrische gegevens in bezwaar zouden kunnen gaan; een beleid dat vooralsnog juist rechtszaken *triggert* en tot allerlei acties van burgergroeperingen leidt.

Overigens zou het biometrische paspoort in één opzicht wel tot meer keuzevrijheid voor de burger moeten gaan leiden, namelijk de (in de wetsgeschiedenis van regeringszijde veelgenoemde) plaatsonafhankelijke aanvraag en uitgifte ervan. Gezien de hogere kosten van het biometrische document valt echter te betwijfelen of de algehele dienstverlening aan de burger hierdoor wordt verbeterd. Hetzelfde geldt in verband met de langere wachttijden bij

Nederlandse gemeenten, de strikte eisen voor pasfoto's en het feit dat Nederlanders in het buitenland voor de aanvraag van een nieuw reisdocument aangewezen zijn op minder ambassades en consulaten dan voorheen (wat voor hen tot langere reistijden en hogere reiskosten leidt). Tevens is het nog maar de vraag hoe groot de groep Nederlanders zal zijn die daadwerkelijk van plaatsonafhankelijke aanvraag en uitgifte gebruik zal gaan maken.

4.6 Identiteit

Opvallend in de Nederlandse geschiedenis van het biometrische paspoort is tenslotte dat alles er (veelal impliciet) draait om het concept identiteit in zijn meest beperkte, kunstmatige vorm: ieder mens heeft hier een 'identiteit' in de zin van een willekeurige verzameling oppervlakkige, digitaal geregistreerde lichaamskenmerken. Zo blijft er van de mens in wezen niet veel meer over dan een biometrisch algoritme. (De mens als – weliswaar uniek – getal.) In dit beperkte mensbeeld lijkt voor de problematiek van gewetensbezwaarden en principiële weigeraars per definitie geen plaats. Dit zou dan ook het gebrek aan keuzevrijheid terzake kunnen verklaren. Invoering van een alternatief, nationaal identiteitsdocument zonder biometrie zou een vorm van erkenning van deze groep mensen inhouden (en daarmee tevens erkenning betekenen van hun identiteit in diepere zin).

Behalve in individuele zin zou men zich ook kunnen afvragen in hoeverre de nieuwe Paspoortwet de identiteit van de Nederlandse bevolking raakt als democratisch collectief van 'vrije' burgers. Immers: door de nieuwe Paspoortwet wordt iedere burger (meer dan voorheen) in wezen beschouwd als potentiële misdadiger of terrorist. Ook verwordt de Nederlandse bevolking als het ware tot een biometrisch transparante massa waaruit zowel individuele leden als groepen ongemerkt kunnen worden geïdentificeerd en doorgelicht, gevolgd en ge*profiled*. Zo niet nu, dan wel in een toekomst (en onder een regering) waarin dit technisch (en wettelijk) mogelijk zal zijn. Naar toekomstige bevoegdheden in dezen kan men nu nog slechts gissen, evenals naar de mogelijke *chilling effects* die dit zou kunnen hebben voor de uitoefening van klassieke vrijheden van beweging, demonstratie, meningsuiting, religie en non-discriminatie en daarmee tevens voor de democratische dynamiek van de pluriforme maatschappij als geheel. Immers, zoals een burger die zich bespied waant zich minder vrij voelt, gedraagt en ontwikkelt, zo zal dit ook gelden voor een biometrisch gemonitorde bevolking als geheel. Het zou dan ook van democratische verantwoordelijkheid en lange-termijnvisie getuigen indien dergelijke risico's wettelijk zouden worden uitgesloten.

